VIRGINIA COMMONWEALTH UNIVERSITY

Virginia Commonwealth University
VCU Scholars Compass

Theses and Dissertations | Graduate School

2004

Meanings of Security: A Constructivist Inquiry into the Context of Information Security Policy Development Post 9/11

Linda F. Larkin
Virginia Commonwealth University

Follow this and additional works at: http://scholarscompass.vcu.edu/etd

 Part of the Public Affairs, Public Policy and Public Administration Commons

© The Author

Downloaded from
http://scholarscompass.vcu.edu/etd/1272

This Dissertation is brought to you for free and open access by the Graduate School at VCU Scholars Compass. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of VCU Scholars Compass. For more information, please contact libcompass@vcu.edu.

CENTER FOR PUBLIC POLICY
VIRGINIA COMMONWEALTH UNIVERSITY

PH.D. IN PUBLIC POLICY AND ADMINISTRATION

This is to certify that the dissertation prepared by Linda F. Larkin entitled:

Meanings of Security: A Constructivist Inquiry Into The Context of Information Security Policy Development Post 9/11

has been approved by his or her committee as satisfactory completion of the thesis or dissertation requirement for the degree of Ph.D. in Public Policy and Administration.

Mary Katherine O'Connor, Ph.D., Chair

David J. Farmer, Ph.D.

Janet R. Hutchinson, Ph.D.

M. Njeri Jackson, Ph.D.

Michael D. Pratt, Ph.D., Interim Director, Ph.D. Program

Robert D. Holsworth, Ph.D., Interim Director, Ph.D. Program

F. Douglas Boudinot, Ph.D., Dean of Graduate Studies

DATE OF DISSERTATION DEFENSE: November 18, 2004

© Linda F. Larkin, 2004

All Rights Reserved

Meanings of Security: A Constructivist Inquiry into the Context of Information Security Policy Development Post 9/11

A dissertation submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy at Virginia Commonwealth University

By

Linda F. Larkin
B.A., Richmond College of the City University of New York, 1976
M.S., Columbia University, 1984

Director: Mary Katherine O'Connor, Ph.D.
Professor, School of Social Work

Virginia Commonwealth University
Richmond, Virginia
November 2004

Acknowledgement

I would like to thank those people whose support, encouragement, and inspiration have sustained me throughout this project.

First of all, I would like to thank my children for their love and for being there for me to love, providing perspective and balance to my life. My daughter, Heather, whose dissertation process has coincided with mine, deserves thanks for listening, for casting me in the role of good example, and for introducing me to the work of Ken Wilber. I thank my son, David, for his moral support, fine cuisine, and most of all, for sharing his perspective and helping me to see things in new ways. Thank you also to my daughter, Diana, for lovingly anticipating my needs, for critiquing my case study, and for offering me the joys of grandmotherhood, in the midst of the dissertation process, by producing a miracle in the form of my new grandson, Charles.

Thanks to my mentor and friend, John Presley, for helping me make space in my life for this dissertation, but more importantly, for his unwavering confidence in me and for an occasional push, just when I needed it.

To my research participants, who experienced this journey with me and contributed to my transformation. Thank you for your perspectives and for helping me to gain an even greater appreciation for the big picture.

To my peer reviewer, Dr. Pam Kovacs, for her thoughtful readings, her wisdom, and for getting excited about my work; to my peer review group, of whom I am the last one left; thanks for showing me the way; and to my auditor, Kate Didden, for asking the hard questions and helping me to clarify my own understanding.

To my committee members, for the guidance that shaped this project: Dr. David Farmer, for helping me to expand my vision and look at risk, the other side of security; Dr. Janet Hutchinson, for opening the door to the knowledge creation piece of this; and to Dr. Njeri Jackson, for discussing technology and society and steering me where I needed to go.

To Dr. Mary Katherine O'Connor, for her wonderful ability to bring out the best in my work, while letting it remain my own. Thanks for your willingness to see the interconnectedness that allowed me to undertake this project and for your inspiration and kindness along the way. I have learned so much from you. It means more than I can say.

Dedication

This dissertation is dedicated to my mother, Susan C. Jamison, whose death in 1995 preceded her dissertation defense. This is for both of us. Thank you for teaching me to appreciate life's complexities and to look for creative approaches. You continue to inspire me and I feel your warmth and your smile.

Table of Contents

List of Figures

Figure Page

Abstract

MEANINGS OF SECURITY: A CONSTRUCTIVIST INQUIRY INTO THE CONTEXT OF INFORMATION SECURITY POLICY DEVELOPMENT POST 9/11

By Linda F. Larkin, M.S.

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University

Virginia Commonwealth University, 2004

Director: Mary Katherine O'Connor, Ph.D., School of Social Work

Security is a term that appears to be used in a variety of ways and to have a number of meanings. In policy discussions, there may be reference to information security, national security, network security, online security, and other kinds of security. In an environment where technological innovation appears to be occurring at an ever increasing rate, policy makers look to technological experts for advice, and information security policy is developed, it seems to be important to consider these variations in meaning.

This constructivist inquiry explores the context in which information security policy is developed and inquires into the meanings, assumptions, and values of those who engage in policy discourse. The guiding research question, "What is the meaning of security?" asks participants in federal and state government, colleges and universities, and the private and non-profit sectors about their understandings of security. The findings of

this inquiry, presented in a narrative case study report, and the implications of this case study provide a richer understanding of the multiple meanings of security in the context in which information is selected and presented to policy makers, advice is given, and policy decisions are made. The multiple perspectives offered by diverse research participants offer valuable insights into the complex world in which information security policy development takes place. While the goal of this research is understanding, the use of thick description in the narrative may aid in the transferability necessary for the reader to make use of this research in other settings. Lessons learned are included, along with implications for policy makers and for future research.

Chapter 1: An Introduction to the Inquiry

Introduction

Security is a term so familiar that we may assume its meaning can be easily understood. On a daily basis, we hear of national security, network security, on-line security, and more. We are becoming familiar with terms such as encryption, firewalls, cookies, and hackers. As we witness technology's capabilities in such areas as surveillance and background investigation, it is easy to see the potential for use with regard to protecting society from crime or attack. At the same time, the recognition of these capabilities seems to create a need for more sophisticated methods to guard our own privacy, as we seek freedom from the danger or anxiety of losing such rights as privacy, free speech, or academic freedom (Etzioni, 1999).

In recent years, the rapidly increasing rate of technological change has created an environment in which those charged with decision and policy making responsibilities often lack the technological expertise to make technology policy decisions without relying on advice from technical experts. Moreover, the September 11, 2001 terrorist attacks on the United States have contributed to a renewed emphasis on security, which also may result in policy makers seeking help from specialists in the field of computer security. Accepting that the incorporation of technical and security issues are important components of the decision making process, technology policy makers are also often guided by professional

codes of ethics or organizational values that are outlined in mission statements or policy manuals. What is the meaning of security for these groups? Who exactly are these experts and what values underlie their assumptions? Is there common understanding or does information security policy development reflect an environment in which some "understand what they do not manage, while others manage what they do not understand" (Spight, 2000).

As discussions occur among those involved with the development of information security policy, it would seem that a discourse in which the notion of security is commonly understood might be necessary if they are to avoid working at cross purposes. Language used in this way allows for meaning to be negotiated and provides a tool for clarifying relationships of people to engineered instrumentalities (Illich, 1973). However, common understanding cannot be assumed to be the sole purpose of language. Language can also be used to present information in such a way as to legitimate a point of view. In this case, power may be maintained through a refusal to recognize the alternate definitions allowed by another discourse (Lyotard, 1984). Further, as issues are framed and presented to policy makers, it is not only language or definitions with which we are concerned, but with the concepts that have been selected to be defined (Postman, 1992). This research focuses on the environment in which information security policy is developed and is concerned with who is involved in policy discussions, what is important to them, how information is presented to policy makers, and asks the question, "What is the meaning of security?"

Security, Technology, and Public Policy: An Historical Context

In 1944, Vannevar Bush, science advisor to Franklin D. Roosevelt, wrote a report entitled, *Science: The Endless Frontier*. In this report, Bush advocated the expansion of the focus on scientific research from its role in national defense to a broader one that called for government support of research to improve the national health and better the U.S. standard of living. In spite of this, defense continued to be a priority in post-war U.S. research and development policies. Bush's recommendations did, however, result in the formation of the *National Science Foundation* (NSF) and the *National Institutes of Health* (NIH). Both agencies have been considered instrumental in the growth of information technology, the NSF for its role in the creation of the Internet and the NIH for developing its web-based medical information resources (Simon, 2000).

With the federal government's concentration on defense, the private sector began to take the lead in the fields of telecommunications and the information infrastructure. At this time the *Advanced Technology Program* and the *Technology Reinvestment Program* became important. The ATP promoted the formation of innovative technology partnerships among federal agencies, large and small companies, universities, community colleges, and local governments (Simon, 2000). The *Technology Reinvestment Program* was set up, through the Department of Defense, to provide grant opportunities to companies interested in re-structuring defense technology programs, thus moving them from the public to the private sector. While the recognition of the importance of technological competitiveness has led to a U.S. technology policy relying on government, university, and industry partnerships, the development of clear and consistent priorities

needed for a successful partnership may be difficult when the goals or values of these groups appear to, at times, be in conflict (Simon, 2000; Tennyson & Wilde, 2000).

Public/Private Sector/University Partnerships

At present, over ninety percent of computer networks are privately owned (Carnevale, 2002). While the emphasis on private development of an information infrastructure has contributed to innovation that might not have occurred in a more regulated environment, it also appears to have led to a re-definition of security that is, at time, at odds with that of the federal government. Encryption technology is an example. As development of encryption has been driven by the advent of e-commerce, improvements in security have dealt with protection of networks from disruption of electronic transactions by illegal means and the protection of individual privacy to support the electronic payment strategies necessary in the Internet marketplace. The government's security image, on the other hand, is concerned with filtering, restricting, collecting, and blocking information flows, should they be seen as a threat to the state (Deibert, 2002; Denning, 1998). Governmental concerns for public safety and widespread use of unbreakable encryption technology have resulted in the Federal Bureau of Investigation's calling this situation one of the most difficult problems confronting law enforcement (Shapiro, 1999). At the same time private information retrieval schemes are becoming even more complex to protect consumers from credit card and identity theft (Wagner, 2001; Gertner, et al, 1998; Dawson, et al, 2002). Private security companies, specializing in advanced encryption technologies, are forming in response to "economic leakage" of web corporations, amounting to an average of 5.7 percent of revenues (Wagner, 2001).

Although it appears that the private and public sectors both derive benefits from partnerships in technological development (Anderson, 2003), they may continue to find themselves at odds over the purpose and use of that technology. An example of this may be the conflict resulting from private sector development of Digital Rights Management System (DRM) in response to changes brought about by digitization. These systems, designed to protect the rights of copyright holders from the theft of their work, by preventing what they call anonymous consumption of information, appear to be counter to the rights of individuals to confidentially access information, as well as those of librarians and educators, who rely on the concept of fair use and an environment of learning and innovation in which cultural production is typified by equity betweens owners and consumers. (EPIC, 2002; Info, 2001; Wagner, 2002). In addition to making no allowance for fair use, systems designed to monitor activity in order to prevent copying of protected works, serve as a form or surveillance tool with regard to what citizens read, listen to, and watch (Shapiro, 1999).

The inter-connectedness or openness resulting from efforts to improve the flow of information can be viewed as a weakness in that cyber-attacks, unlike traditional military attacks, can be directed at privately owned information networks and can be just as effective a weapon as military force. For this reason, some in the public policy arena claim that U.S. policymakers' concept of national security has not caught up with the new threats of computer warfare and call for Congress to pass legislation allowing for tracking of intrusions on the Internet and permitting law enforcement agents to infiltrate computer networks (Adams, 2001). At the same time, others see protection of traditional

expectations of privacy as a challenge for policymakers, when it is desired that consumers fully participate in e-commerce and the high tech marketplace and personal information is seen as essential for continuing to offer consumers the full range and quality of services they have come to expect and enjoy (Gregoire, 2002). While encryption technologies and other technological devices have been used, with varying degrees of success, by individuals seeking to protect their privacy from governmental intrusions, attempts to monitor and control Internet behavior may have had a chilling effect on in the marketplace, e-commerce, e-business, and elsewhere where trust and assurance of privacy are required (Albarran & Goff, 2000; Franda, 2002).

When an Office of Homeland Security was formed in the aftermath of the September 11, 2001 terrorist attacks to strengthen US security and eliminate the vulnerabilities to the critical infrastructure exposed by the attacks, recommendations were made to state agencies to work with their federal counterparts to develop security standards for infrastructure protection and information sharing (Heritage Foundation, 2002; Office of Homeland Security, 2002). As critical targets were identified in response to steps outlined in the *National Strategy to Secure Cyberspace*, colleges and universities became recognized as potential targets for terrorists launching cyber attacks from school computers. At the same time, university information officers were charged with addressing best practices in the technology of information security and establishing information sharing and analysis centers (President's, 2002).

As universities begin to compete for federal grants to develop surveillance and counter-terrorism technologies, they also appear to be concerned about threats to

confidentiality and invasions of privacy that they view as antithetical to the traditions of academe (Carlson & Foster, 2002; Olsen, 2002). An example of this traditional view can be found in a statement on the *State Council of Higher Education in Virginia* web-site, outlining a policy by which personal information about citizens is only collected to the extent necessary to provide service and that citizens will understand the reason for the collection of information about them and be permitted to examine it (SCHEV, 2002). However, it is also common practice for universities to regularly monitor use of resident students in order to prevent threats to their computer networks (Golick, 2000). Concern over these conflicting priorities has led to research into some of the ethical and legal dilemmas highlighted here. Currently, the *National Institute of Standards and Technology* is funding a project at George Mason University's *National Center for Technology and Law*, studying the legal difficulties of guaranteeing the security of computer networks (Carnevale, 2002). In 2001, the Commonwealth Information Security Center at James Madison University was also formed to conduct technological and policy research and make recommendations to policy makers (CISC, 2002).

With the passage of the *Cyber Security Enhancement Act of 2002* and the inclusion of a distinct role for U.S. universities in the *Homeland Security Act of 2002,* it could be that the higher education setting is uniquely situated to provide a neutral platform that can help to foster joint network security goals for academia, government, and private industry (Borrego, 2003; Carnevale, 2002). If we are to consider the multiple definitions of security and technology that are presently being used, along with the multiple perspectives of the various levels of government, private industry, private citizens, and the academic world, it

appears that there may be something to gain from an analysis that will clarify positions and aid in the development of a dialogue. Debate over issues surrounding the development of information security policies can be seen as having moved from a more philosophical or ideological realm to a public forum, as citizens react to recent acts of terrorism or to governmental responses to terrorism. What had been concerns over such things as the freedom to access information or the right to personal privacy, now seem to have taken on an element of public safety and government intrusion, as positions articulated by political actors and the media appear to become more polarized. As policy makers attempt to develop policy that assures our freedoms, while guaranteeing public safety and considering such concepts as equity, they not only encounter those with widely varying perspectives, but may also encounter points of view based on entirely different assumptions and definitions from their own. This is all the more evident in the area of information security and technology, where technological language continually evolves to keep pace with technological innovations and applications.

In *Against the Gods*, Peter Bernstein (1998) explored the role of risk in society and concluded that, while history may repeat itself, it only does so imperfectly, as conditions can never be repeated exactly. As he points out, computers only answer the questions, they don't ask them and that whenever we ignore the truth, computers will support us in our conceptual errors. What appears to be important here is not that technological discourse is wrong or that policy makers are incorrect when they look to the past to determine a course of action, but that when multiple perspectives and multiple meanings exist, any discourse that ignores that may prove ineffective in assessing risk or in

developing policy. If conditions can never be repeated exactly, then the context within which policy development occurs would seem to take on added importance. "The imaginations constitute the place of history and the 'progress of language'" (Derrida, 1980, p. 78).

The Context of the Inquiry

In August, 2002, Virginia joined with Maryland and the District of Columbia in the *National Capital Region Summit on Homeland Security*, agreeing to work in partnership to coordinate plans for terrorism and security-related training and exercises across the national capital region, including all levels of government, colleges and universities, health care institutions, and partners from the private and non-profit sectors (National, 2002). Prior to this, former Virginia Governor Gilmore spoke of cyber terrorism as not solely a federal issue, but one that required public and private cooperation ("Advisory Panel," 2000). That same year, a report prepared for the Virginia Center for Innovative Technology by the Mason Enterprise Center and Institute for Public Policy at George Mason University identified information security and biometrics as important information technologies in Northern Virginia (Stough, Kulkarni & Trice, 2000). Section 882 of the Homeland Security Act of 2002 established an *Office for National Capital Region Coordination* and recognized the particular vulnerability of Virginia, Maryland, and the District of Columbia to acts of terrorism (H.R. Rep. No. 5005, 2002). Likewise, Virginia's official document on Homeland Security strategy identified Virginia's unique geographic location – as home to the world's largest naval base, as a hub for Internet traffic, and as a neighbor to the nation's capital as justification for federal funding (Hager, 2002). By its

accessibility, my own familiarity with the context, and a stated commitment to the development of security strategies in partnership with the federal government, the Virginia/ DC area offered a unique setting for research into the interaction among state and federal policy makers, the private sector, universities, and other stakeholders in information security policy development.

Set within a framework in which public policy is developed; this inquiry is not concerned with policy evaluation or comparison. What is of interest here is the interaction among the actors in this arena, as their varying language, assumptions, frames of reference, and perspectives bound the context in which decisions about information security are made and policy developed. The literature review in chapter two provides more detail about what shaped my thinking about this topic that led to the development of a researchable question and chapter three both offers a theoretical basis for my use of an interpretive paradigm and its suitability for this research and demonstrates how the research design emerged through a hermeneutic dialog in which I was actively involved with the other participants.

Interpretations and Implications of the Data

The narrative case study, which comprises most of chapter four, represents the perspectives of the twenty-five participants in this study, as well as my own perspective as the researcher. Using a conference environment as a background, composite characters engage in a series of panel discussions. Through the use of thick description in the case study, I attempt to contribute to clarity by offering a way for the reader to step into the context and experience it along with the participants and myself (Bouma & Atkinson,

1995; Lincoln & Guba, 1985; Rodwell, 1998, Zeller, 1999). In an introduction to the case study, I discuss the responsibility of the writer of the case study to honestly and accurately portray participant perspectives in the context and the responsibility of the reader to fully engage in the process of reading so that relevance and, ultimately, the usability of the research can be determined (Guba & Linclon, 1981; Rodwell, 1999). I also spend some time discussing my difficulty in developing a conceptual map of the relationships in the complex environment inhabited by the research participants and how I was aided in this struggle by using Ken Wilber's integral approach to consider each piece of data in terms of a four quadrants, thus allowing me to depict the intersubjective, subjective, behavioral, and structural nature within each stakeholding group (Wilber, 2000). It is my hope that this map will serve as a useful tool for readers in making meaning of the case study.

Conclusion

It has now been over three years since the 9/11 terrorist attacks on the United States and the 9/11 Commission has criticized the president for not taking threats seriously enough (National Commission, 2004). As we hear about the possible threats of cyberterrorism to the critical infrastructure of this country and policymakers must make security decisions in a technological environment, it seems to be important to consider the challenges for policy makers attempting to identify threats and find resolutions within a bureaucratic context. Attention to the complexity of the environment seems called for, both in light of responding to unknown threats and in assuring that public safety does not overshadow privacy rights, freedom of information, and other values and interests competing for the attention of policy makers. As partnerships are formed between

government and industry and universities apply for government grants, there may be conflicting interests. While some might say that these are easy choices in times of crisis, others might counter that oversimplification is not only unnecessary, but dangerous. This inquiry examines the perspectives and priorities of policy makers and other stakeholders in information security policy development in an attempt to provide a better understanding of this complex environment, the relationships that exist within it, and what implications these have for policy development.

Chapter 2: A Review of the Literature

Background

An understanding of policy discourse involves the recognition of a political element that seems to deny the existence of one absolute truth. Rather, a number of truths appear to exist, from which those engaged in discourse can select. From a point on this spectrum, a political actor may participate in a discourse that involves choosing a particular truth. This takes place whether genuine discourse or only monolog, disguised as dialog, is occurring (Buber, 1958; Fox & Miller, 1996). In selecting among competing truths, policy makers may also shape how we interpret and understand that truth (Anderson, 2003). In this light, some background in the discourse surrounding current policy issues in the area of security and technology may provide some insight.

The concept of private security, or concern with protection of the privacy of the individual from the state, has traditionally played an important part in policy development in the United States. With the increased ability to track Internet activity, create electronic profiles of individuals, and raise the level of surveillance, security policy responses have focused on such issues as protecting personal data and deregulating encryption technologies (Deibert, 2002). This can be contrasted with network security, which is concerned with protecting networks from data corruption and disruption in the flow of information. Policy responses, when the primary object of security is the network, include

the development and use of intricate systems of encryption technology and secure access. What may be most significant, however, is that policies associated with the network security collective images are oriented in precisely the opposite direction of those traditionally associated with the term security (Carnevale, 2001; Deibert, 2002). It is possible that, as the density of information networks increases, a network security image may become dominant as other security images are constrained (Deibert, 2002). Such a change in focus could result in a corresponding shift in political power, as the control of territory is replaced by control of information flow (Singh, 2002).

As policy discussions about information security occur and partnerships among universities, private sector, non-profit, and government agencies take place, it may be important to look at the range of truths from which policy makers are selecting and to consider the perspectives they represent, whether there is common understanding, how priorities of those involved in the discussion might influence policy decisions, what underlying values may be in conflict and, if so, whether true discourse and deliberation are desired or a specific end is seen to justify the means. While the context studied here is a complex one that could be divided up in a number of ways, my approach to the literature reflects my working hypotheses:

- *H1*: Policy makers rely on technological experts in the development of information security policies.
- *H2*: Policy makers and technological experts often use different terminology.
- *H3*: Values underlying assumptions for these two groups are different.

This review of the literature sets the stage for my entry into the context of information security policy development, the emerging research design, the case study and, finally, lessons learned.

Security, Language, Values, and Framing

The importance of language to public policy can probably be most simply understood as the link between the development of a policy and its articulation (Hult & Walcott, 2001). However, the way words are defined, which words are chosen for definition, and the values underlying those words all play a role in policy discussions, as does the way information is presented and to whom and by whom it is presented. The presence of ambiguity in political discourse, if acknowledged, may actually be useful (Timura, 2001; Zahariadis, 2003). Timura (2001) points out that ambiguity in an emerging discourse can help to generate a conversation incorporating diverse points of view. It is not only important to focus on what is being said, he adds, but on who is saying it, so that perspectives from multiple research communities can participate in further definition. By doing so, we acknowledge that dialogue is more than mere talk, but is perspectivism taken seriously (Farmer, 2002). The recognition that ambiguity exists can allow for issues to be framed in ways that can help to make particular policy outcomes more successful. For example, when people are not sure what they want, describing the issue in terms of a gain or a loss may significantly alter a policy outcome (Levy, 2003; Zahariadis, 2003). The same can be said for using emotion or analogies in framing. In this way, meaning is clarified, whether or not the particular issue can be resolved (Zahariadis, 2003). Taking this further, an acknowledgment that ambiguity exists may allow for new models for

policy deliberation to be adopted. Rather than each being oriented toward their own success, participants could pursue individual goals under the condition that they coordinate action plans on the basis of shared meaning. By viewing other participants as equals and entering deliberations with a willingness to change their own views, argumentative persuasion can take place without coercion (Gutmann & Thompson, 1996; Risse, 2000).

John Walsham (1990) considers computer information systems from the metaphorical perspectives used by Gareth Morgan to study organizational image. These eight metaphors allowed organizations to be viewed as machines, organisms, brains, cultures, political systems, psychic prisons, flux and transformation, and instruments of domination. By recognizing that common understanding of organizations is often based on metaphor and that this kind of understanding tends to be one-sided, Morgan's framework offered an approach to organizational analysis that allows for complexity (Morgan, 1986). Walsham (1990) suggests that applying these same theoretical perspectives to computer information systems will result in a more pluralistic approach to information systems research and a decreased emphasis on the mechanistic and organismic understandings of organizations.

Acknowledging the limits of a particular discourse can help to increase its benefit to the user, as this allows him or her to temporarily adopt different sets of definitions and values with which to view a specific problem, while excluding others (Farmer, 2000). This inter-changeableness may aid in consensus-building by offering decision-makers an opportunity to try on a variety of frameworks, without having to first alter their own personal value systems. A recognition of multiple perspectives can encourage dialogue

among those involved in decision or policy making and help to render the discussion more relevant and useful (Balfour & Mesaros, 1994, Farmer, 1998).

Adopting other perspectives may not only enable decision makers to identify assumptions associated with various paradigms, but also may allow them to locate their own frames of reference and to recognize the appeal of particular theories, approaches, and practices (Netting & O'Connor, 2003). While proposals that do not conform to the values of specialists in policy communities are unlikely to be adopted (Zahariadis, 2003), long standing attitudes, traditions, and beliefs may be based on values that are hidden even from those who possess them (Cowan & Todorovic, 2000). It is through an awareness of the co-shaping of multiple perspectives used that light may be shed on bureaucratic structures, making them more comprehensible (Farmer, 1999). Although policy controversies can be viewed as disputes over conflicting interests, it is the frames held by those involved in decision making that determine what they see as their interests and upon which they will act (Schön & Rein, 1994). Consideration of context may also aid in the interpretation as it provides a way to link data with purpose (O'Connor, 2000) and to integrate previously separate entities and their functions (Beck & Cowan, 1996). Dialectical confrontation between technical experts and generalists can sometimes bring out unstated assumptions and conflicting interpretations of facts and risks concerning a proposed project (Majone, 1989).

Network security, which focuses on protection against data corruption and maintenance of the system, has become a dominant theme in discussions of information security policy. While this mode of thinking, rooted in a functionalist paradigm (Burrell &

Morgan, 1979) focuses on the process, there does appear to be some evidence that information security system policy development may be moving away from this strictly objectivist approach to one that incorporates subjective understanding of social situations. This may be in light of a new recognition of the importance of social implications of computer information systems (Dhillon & Backhouse, 2001). As more attention is paid to cultural and informal aspects of information handling, a functional definition of language that assumes a knowledge of all that is possible to say can be replaced by one that attempts to include all that one wishes to say (Day, 2001). In this way concepts not defined in the technical discourse of network security can be included. A more holistic or integral approach would then include consciousness and subjective well-being as well as the economic, social, and material (Wilber, 2000).

Structural power need not be concerned with empowerment, but with the ability to effect rules and institutions that govern outcomes. When technologies are viewed as structures that demand restructuring of their environments, a reciprocal relationship is revealed (Singh, 2002). Singh (2002) discusses three notions of structural power: one where technologies shape institutions, one where institutions determine technological use, and one where institutions and technology shape each other. This last concept, which recognizes the importance of the role of context both in the development of structural power and in its eventual outcomes is particularly relevant to this study, as the constructivist inquiry assumes that reality is context-based and constructed through intersubjectively achieved meaning (Rodwell, 1998). This approach sees change occurring by means of the interaction between structure and process and the outcome of interplay

among historical, processual, and contextual factors (Dhillon & Backhouse, 2001). In addition to a seeming shift from a functionalist or mechanical philosophy to a more interpretive one in information system security, language and symbols are also becoming recognized as important elements by political scientists. Meaning and form of expression, including the framing of narratives, are seen to demonstrate the coexistence of multiple realities as new words appear to generate new realities while new realities generate new words (Luke, 1994).

The concept of "frame of reference" in policy research recognizes that, participants in policy discourse ascribe to sets of assumptions that cause them to talk about policy decisions or recommendations in particular ways (Carragee & Roefs, 2004; Frisch, 1993; Kanner, 2001; Schön & Rein, 1994). Current research in the areas of framing and risk analysis suggests that organizational decision makers often base courses of action on scenarios generated within a political framework, resulting in their non-participation in problem definition (Kanner, 2001). In that framing involves placing observed events into a context that gives them meaning (Zahariadis, 2003), reliance on others to frame a particular problem and determine relevant information for consideration can limit the courses of action in ways that leave out the specific beliefs of the decision maker (Kanner, 2001). Further, depending on the way that alternative courses of action are presented to decision makers, disparate but equally valid assumptions and rules may be applied to a decision (Kanner, 2001; Frisch, 1993). As bureaucratic expertise is replaced by policy advice from those outside the traditional policy making sphere and technical or private

sector actors become involved in policy implementation, there may be implications for policies whose aim is promoting the public interest (Kobrack, 1998).

People tend to respond to situations as they interpret them, not as they exist in some objective reality (Carroll & Johnson, 1990) and convenience can be a determinant of both source and method for receiving information in a decision maker's frame of reference (Hutchinson, 1996). Advising decision makers involves creating a story that weaves together facts and values (White, 1992). In an environment where decisions are often made quickly, in-person communications with colleagues and professional contacts are regularly used by policy makers to determine answers in difficult policy matters. This suggests that creation and use of knowledge are context bound, highlighting the need for methods to study interpretation of the meaning of events (Hutchinson, 1995).

In security debates, language is often used to describe and consider social questions in terms of crises, threats, and dangers. By considering immigration as a security question, for example, the mobilization of particular institutions, such as law enforcement, is facilitated. In this way, language becomes a defining force in which arbitrarily defined threats can be viewed as being linked, while questions as to their legitimacy can be transferred outside of the security discourse (Huysmans, 2002; Menjivar & Kil, 2002). Strategic frame analysis, designed to help progressive groups advance environmental and other causes, provides insight into public prejudices, allowing them to present facts in a way the public can accept (Mooney, 2003). Framing, then, can be viewed as an extension of an agenda-setting process (Carragee & Roefs, 2004).

With regard to information security, the use of information and communication technology (ICT) may be transforming traditional organizations into bureaucracies where system analysts and software designers are the key decision makers, responsible for programming that reduces the scope of administrative discretion (Bovens & Zouridis, 2002). As information technology (IT) departments assume more decision making responsibility for information security, policy makers are advised by technologists, and government agencies employ private sector software companies for information security solutions, it seems important to take note of this shift in power and consider what it might mean for future information security policy development.

The Interplay of Technology, Security, and Society

In *The Technological Society*, Jacques Ellul predicted a world in which society would develop in response to the needs of technology or *technique* (Ellul, 1964). Similar to Max Weber's argument, years earlier, that bureaucratization is a natural outgrowth of technology (Weber, 1958), Ellul also adopted a definition of technology that equates it with industrialization. However, there are currently some other very different definitions of technology in use that, depending on which is adopted, allow for very different kinds of discussions about technology.

Along with the definition of *technology as industrialization* that has been used by Ellul, Weber, and others, *technology as instrumentality* and *technology as novelty* have been identified as two concepts illustrating typical and implicit understandings of technology (McOmber, 1999). Rather than viewing technology as an impetus to societal change as Weber and Ellul did, technology defined as instrumentality accords it with the

status of a tool or instrument for achieving a specific goal and, thus, serving society. The notion that we can "harness science and technology in support of homeland security," (Office of Homeland Security, 2002) for example, seems to be based on the assumption that technology is subject to our will and can be used for our own purposes to achieve specific ends. Technology as novelty, on the other hand, refers to only the most recent developments of these instruments and is optimistic in its predictions that new technology eliminates all the problems of whatever it replaces. In his address to the *GovNet 2002* Summit in May 2002, Deputy Assistant Secretary for Technology Policy, Chris Israel (2002) stated, "the best minds in the technology industry agree with Governor Ridge and tell us that technology can solve many if not all of our security problems." This view of technology focuses on its ability to eliminate all of the problems associated with whatever it replaces without addressing the idea that new problems may be created by the technology (McOmber, 1999). While it may be useful to discuss the technological revolution in positive terms by adopting a *technology as novelty* definition or to use *technology as industrialization* to draw attention to the problems it creates, it seems clear that each of these definitions taken alone only allows us to see part of the picture. One reason it may be difficult to institutionalize debate in areas of policy making involving technology is that issues under discussion are not always purely technical or purely political (Majone, 1989). Nevertheless, not all areas of discourse are equally penetrable (Foucault, 1972). A principle feature of technological discourse is that it often isolates technology from the societal circumstances of its origin (McOmber, 1999). Martin Rein (1973) points out the need for intermediaries who can effectively relate the four

autonomous segments of a highly interrelated system: policy making, technological innovation, administrative practice, and research.

As technological innovations are applied to problems of information security and these and other assumptions about the purpose of technology become the basis for making decisions, it is possible that operational definitions and strategies implemented may be limiting. S*ecurity*, another term not easily defined, seems to imply that there is something in need of securing or "making safe" and that it is possible to do that. In a complex environment this goal may become problematic (Glokany, 2001; Jentleson, 2002; Pauchant & Mitroff, 2002; Ravetz, 2003; Wise, 2002). Information security policy will reflect the views of those who are involved in policy discussions and what problems they are trying to solve. Research in this area focuses on data protection and e-commerce, individual privacy, ethical issues of information privacy, electronic governance, encryption, information sharing, surveillance, academic freedom, critical infrastructure protection, and risk assessment.

E-commerce approaches to information security primarily deal with protection of data and consumer's personal, financial, or transaction information (Miyazaki & Fernandez, 2001). However, intergovernmental and public/private partnerships are seen to play important roles in and have implications for homeland security and public safety ("Big Picture," 2003; Vaida, 2002). Along with issues of anonymity and privacy, surveillance and security are becoming recognized as compelling frames for public discourse concerning electronic payment systems (Phillips, 1998). While cryptographic research conducted at universities, such as the SPIR (symmetrically-private information

retrieval) model developed by the University of Pennsylvania, MIT, and the University of Haifa, focus on guaranteeing both the privacy of the data and the privacy of the user (Gertner, Ishai, Kushilevitz & Malkin, 2000), recent government sponsored research supports development of tools for surveillance and the development of databases for information sharing of data about individuals.

Carnivore and "packet sniffing" software have been developed by the FBI to combat terrorism, espionage, and other felonies by intercepting electronic communication and downloading a broad range of data within the context of searching for court ordered information (Nelson, 2002). This comes along with a gravitation toward digital surveillance, which is to eventually include biometric features, mug shots, and video images (Safir, 2003). *Control Web*, a second Internet built into the network environment and made possible by the convergence of technology, will allow for greater control of access by making use of biometrics and linking up with drivers' licenses, tax records, etc. (Internet, 2002). Two other recent technological innovations developed for use in anti-terrorism efforts are RISS (The Regional Information Sharing Systems Program) and MATRIX (Multistate Anti-Terrorism Information Exchange). RISS was recently expanded to include ATIX (Anti-terrorism Information Exchange), a Justice Department Initiative that will link thirty-two types of federal, state, and local public safety organizations ("V-One Corporation," 2003). MATRIX, a federally funded pilot project, operated by the Florida Department of Law Enforcement, was begun after the September 11th attacks and contains public records from thousands of locations on U.S. individuals and businesses ("MATRIX History." n.d.)

In the United States privacy law, encompassing one's right to control his or her personal information, the right to make autonomous choices, and the right to be free from unwarranted intrusion, is still evolving (Strickland, 2002). The problem of the "unobservable observer" may be an insoluble one and, as such, a challenge for lawmakers as they consider how much privacy we are willing to surrender for public safety (Goold, 2002; Rothkopf, 2002). Researchers at Georgetown University, considering information privacy to be one of the most important ethical issues of the information age, have developed an instrument that identifies and measures dimensions of individuals' fundamental concerns about organizational information privacy practices and call for future interpretive research into the meaning of information privacy for individuals within an organizational context (Smith, Milberg & Burke, 1996). A Canadian study focusing on electronic governance in five countries indicates that privacy is emerging as an important international issue. When the abuse of personal information and increased scrutiny of citizens are viewed as negative consequences of electronic governance, more emphasis is placed on privacy as a broad right in a cultural, as well as a legal sense (Riley, 2000).

U.S. public policy has, traditionally, exhibited a balance between concepts such as privacy and individual freedom, on the one hand, and public safety and the common good, on the other. This balance may be complicated when these concepts are understood in particular ways and we attempt to assign specific meanings to them (Farmer, 2002). It is possible that, in doing so, we narrow the range of possible policy alternatives and find ourselves in a position of having to choose between two outcomes that appear to be mutually exclusive. For example, by allowing ourselves to be persuaded that technological

invasions of privacy are necessary to preserve the common good, we fail to accord status to the concept of individual liberty (Nelson, 2002). Consideration of whether or not privacy is a realistic expectation in the twenty-first century may, to a great extent, depend on public perception. Although the Internet provides a forum for citizen discussion and involvement, the willingness to organize and act so that government and private industry will respond to demands for privacy may not occur unless the public actually believes privacy is attainable (Berman & Bruening, 2001). It is possible, as public surveillance becomes more and more commonplace, that individuals may begin to surrender expectations of privacy (Goold, 2002). Citizens in the United States not only have very little control over the data that has been collected about them, they also know very little about the kind and extent of the kinds of information others have access to. This situation may exist because of the way issues have been framed and the problem defined. By discussing information privacy as a consumer problem rather than a societal concern, responsibility for protecting personal information has been left to the individual rather than resulting in the oversight that might have occurred if a resolution had been sought in the public interest (Nehf, 2003).

Assessing Risk

On October 16, 2001 President George W. Bush issued an executive order, *Critical Infrastructure Protection in the Information Age*. This document called for cooperation among federal and state governments, the private sector, and academia to protect the critical infrastructure (Bush, 2001). IT infrastructure consists of the Internet, telecommunications, embedded real time computing devices such as systems for aircraft

control and SCADA (Supervisory Control and Data Acquisition) systems controlling electrical energy distribution, and desktop computers. In addition to prevention, detection, and mitigation of terrorist attacks, the IT industry is seen as playing a major role in protecting this critical infrastructure through the aggregation of data from multiple sources for purposes of information sharing and gaining insight into terrorist plots (Committee on Science and Technology, 2002; H.R. Rep. No. 5005, 2002; National Strategy, 2003; Wong, 2002).

In his 2003 budget, President Bush increased the Commerce Department's Technology Administration budget in order to promote innovation through policies encouraging research, development, and commercialization of new technologies and to support entrepreneurship through policies promoting technology-led economic development (National Institute, 2003). Two years earlier presidential cyber security advisor, Richard Clarke, had warned of an "electronic Pearl Harbor" and called for strengthening security for safeguarding the nation's critical infrastructure (McGuire, 2000; National Commission, 2004). Private industry's approach to information sharing appears to have been largely technical, seeking greater return on investment and improved security for IT assets ("Virginia's Technology," 2003). Important challenges for the private sector included system architecture, protecting organizational data, and the use of varying definitions by different agency cultures involved, such as the CIA and FBI (Carey, 2003). While it could be argued that it is not the role of the private sector to concern themselves with broader societal implications or competing claims for protection of critical infrastructure, information sharing, and surveillance, on the one hand, and individual

privacy or freedom of information, on the other, this oversimplification or narrow interpretation of the context could result in information security solutions that become problematic in their implementation in public sector institutions and, ultimately, for the public at large. Recognizing that technological expertise cannot be relied upon to uncover the inherent risks and social implications of new technologies (Majone, 1989), John Marburger, Director of the White House Office of Science and Technology, commented after the September 11th attacks that the social sciences may have more to offer us on the difficult problems of our time than we are acknowledging (Anderson, 2003).

Aside from concern that those working on solutions to information security problems may not have made efforts to include a broad range of perspectives, there may be other dangers to ignoring the complexity of the environment. As technology becomes more sophisticated, it not only provides faster and easier methods for securing information. It also increases the possibility for unexpected consequences. Considered in this way, efforts at risk management appear to be somewhat paradoxical in that information cannot be secured one hundred percent and success is seen in terms of preventing some unknown occurrence from happening (Ravetz, 2003). At the same time IT costs continue to climb and financial considerations seem to dominate decision making about IT projects (Earl & Khan, 2001).

An approach to risk management that focuses on profitability and simple problem solving within a bureaucratic context and does not address problems that are complex and defy resolution may not be viable in the context of terrorism, which can be described as both creative and destructive (Hovden, 2004; Pauchant & Mitroff, 2002; Wise, 2002). *The*

U.S. Domestic Preparedness Program, which was created in the mid-nineties to prepare the United States for destructive terrorist acts, may have left the United States ill prepared for the September 11th terrorist attack on the World Trade Center by relying too exclusively on a disaster management approach (Falkenrath, 2001). Effective risk management strategies must also attend to this destructive side of complexity. It is possible that, by focusing too little on anything nonbureaucratic or nonsystematic, traditional public administration discourse can fail to give credence to the importance of interconnectedness with ideas outside the discipline. This unwillingness to broaden their focus may have resulted in U.S. policy makers failing to recognize the symbolic nature of the World Trade Center, which made it a terrorist target (Farmer, 2002; Naim, 2002). A more far-reaching focus and the inclusion of multiple perspectives in information security research might allow for the human interpretation (White, 1986) of computer-based information systems necessary to better understand and respond to a complex environment. By acknowledging that the complexity of the context and recognizing the ambiguity cannot be resolved, policy makers may be able to come closer to making the process comprehensible (Zahariadis, 2003).

While risk assessment and information security policy response in a context of terrorism may only yield temporary and imperfect solutions (Wise, 2002), they may allow for a more critical appraisal if desired outcome and the potential harm of a policy are considered together. In this way, for example, threats could be ranked by nature, magnitude, immediacy, uncertainty, and persistence and then increased or reduced in light of the policy under consideration (Glokany, 2001). In their research on “dark networks,”

Raab and Milward (2003) compared the Al Qaeda network to a corporation with a functionally differentiated core that financed and supported terrorist cells by coming up with ideas and plans for action. As integration of functionally or geographically differentiated elements is necessary to be successful, then an appreciation for the network's complexity would more easily allow for identification of links and disruption of the activity of the network. Likewise, a decentralized model might prove superior to a hierarchical one in responding to and managing emergencies in an unstable environment (Wise, 2002). In the area of military strategizing, for example, it has been argued that consideration of biological agents is not useful, as they are unpredictable and too dependent on other uncontrollable factors. Yet, that is exactly what would make them appealing to terrorists (Ostfield, 2004).

It is possible that by redefining counterterrorism to respond to the threat posed by Al Quaeda, the United States would have been better prepared for the September 11th attacks (National Commission, 2004). Unlike classical terrorism that targets political adversaries and is aimed at the institution or a political program, what can be described as a new brand of terrorism appears to be both destructive and elusive (Diken & Lausten, 2004). However, the notion of preventing terrorist acts that have not yet taken place, may raise additional concerns. While the Bush administration's War on Terror focuses on identifying and stopping terrorists before they can act, this strategy appears to be problematic from a global perspective (Diken & Lausten, 2004; Chomsky, 2003a). If potential threats are limitless (Chomsky, 2003a) and states that harbor potential terrorists are subject to attack by the United States (Chomsky, 2004), then virtually any nation in the

world may be at risk. This appears to be creating some uneasiness internationally. Rubens A. Barbosa (2003), the ambassador of Brazil to the United States, ascribes changes in the post 9/11 world not to specific acts of terrorism, but to the demonstration of power by the United States. This demonstration of power was also felt in the Middle East, when the U.S. perception of Gulf States as enemies appeared to threaten their political culture (Sayegh, 2004).

In addition to increasing international concern about what some describe as imperialistic U.S. practices (Barbosa, 2003; Chomsky, 2003a; Diken & Lausten, 2004; Foster, 2003; Gwyn, 2003; Kelly, 2003) come concerns that, rather than deter terrorists, what appears to be a muscle flexing U.S. stance may actually increase the likelihood of terrorism. The War on Terror may increasingly be viewed as a pretext for intervention and atrocities (Chomsky, 2001b; Chomsky, 2002a) with no prospect of ever being won (Byrne & Weir, 2004). It is possible that the waging of a preventive war and the use of a definition of terrorism that focuses on who is the subject of attack rather than on the nature of the acts themselves may allow the United States to engage in exactly the kind of attack on other nations that they seek to prevent (Chomsky, 2002). Further, with a policy aimed at preventing terrorism before it occurs, it may be difficult to know whether the action taken was preventive or an act of terrorism in itself. International law confines the use of force to self defense (Byrne & Weir, 2004). Although condemned for international terrorism by the World Court, the United States continues to portray itself as justified in reacting to inflicted wrongs (Kelly, 2003) and, while U.S. citizens may search for a useful moral or valuable lesson (Rosin, 2002) in the events of September 11th, it may also be

important to reflect on how fairly standards we apply to others have been applied to ourselves (Chomsky, 2001; Chomsky, 2001b; Chomsky, 2003). What's more, it may be appropriate to ask why policies are couched in terms of what we are against rather than what we stand for (Ash, 2003) and what this means in terms of assessing risk.

As the international community notes what appear to be double standards in policies of the United States (Chomsky, 2001a; Chomsky, 2003b; Sayegh, 2004) and a forceful assertion of military power, other alliances are formed to counterbalance it (Ash, 2004; Kux, 2002). Jentleson (2002) finds scholarship in political science and public policy little help to policy makers, in that it is too theoretical and does not call for greater praxis to be pursued as a step to fulfilling broader societal responsibilities. If policy makers cannot assess the nature of the problems they face, they may continue to be ill-prepared to develop relevant policy in response to terrorism. However, the problem may not be in taking a theoretical approach. The challenge for those in policy research and discussions may be in their ability to reenvision theory and make it relevant for application in this particular context (Miller & King, 1998).

Government/Private Sector Security Solutions

After the September 11th attacks, some citizens and legislators began lobbying for a national identification card system as a means for verifying identity of people boarding planes, entering the country, and reducing the threat of terrorism (Porcelli, Selby, Tantono, Bagner & Sonu, 2002; Schulman, 2002). At around the same time, the Justice Department closed immigration hearings of foreign nationals, citing national security concerns (Baker, 2002). This resulted in a ninety-five percent reduction in refugees admitted to the U.S. in

the first quarter of 2002 (Donovan, 2002). *The Homeland Security Act of 2002* also tightened restrictions on the issuance of visas and gave authority for procedures for the issuance of student visas to the *Office of Science and Technology Policy* (Office of Homeland Security, 2002). *Bill S. 3076*, introduced by Virginia Republican senators, John Warner and George Allen in October 2002 exempted government contractors from liability involving technologies and services sold to the government for Homeland Security purposes (S. Rep. No. 3076, 2002). With legislation calling for cooperation between the public and private sectors, tax breaks for firms developing cyber security products, and a current Homeland Security budget of over thirty-one billion dollars (H.R. Rep. No. 5069, 2004; H.R. Rep. No. 4852, 2004), it may not be surprising that some of the most outspoken proponents of such measures are CEO's from computer firms specializing in security solutions (Schulman, 2002; Williams, 2002) and that new security companies are arising to meet the demands for more and better technology (Rothkopf, 2002; Wagner, 2001). Private sector interest in security may be more than an entrepreneurial one, however. Citing political constraints on government action as impediments to development of effective systems security, McCrohan (1998) suggests that involvement of businesses, unhindered by such constraints, is necessary for the United States to maintain information superiority over its enemies.

While objection to national identification cards and SEVIS (Student and Exchange Visitor Information System) have come primarily from those with concerns for privacy and due process, there are also those who question the effectiveness of these systems in keeping us secure (Celko, 2002; Relyea, 2002; Schulman, 2002). SEVIS procedures, for

example, have been outlined in a simple five step process (Verton, 2002). However, as a purely technical solution to a security problem, the danger may be in its inability to address the complexity of a problem that is multi-faceted and continually transforming. In a speech to the Heritage Foundation in September 2003 Robert Bonner, the Commissioner of the Bureau of Customs and Border Protection at the Department of Homeland Security declared America safer and our borders more secure against terrorists than they were in 2001 (Bonner, 2003). Unless the environment remains static, however, it may be difficult to know for sure. It's possible that security functionality may more accurately be gauged by studying the interaction between changing volume and velocity of violence capability in various contexts along with capability of competing security methods to constrain violence (Deudney, 2000).

Along with concerns that technological development for security may not be taking important factors into account, such as birth certificate fraud prior to obtaining ID cards or maintaining accurate and up to date information in databases ("Dangerous Data," 2004; Schulman, 2002), there is recognition that the U.S. may be denying due process to foreign students and immigrants (Baker, 2003) while not acknowledging that illegal immigration often does not occur at the border, but when people overstay their visas (Garrett, 1998; Schulman, 2002). With the advent of electronic reporting of information about foreign students and anti-terrorist legislation, such as the *USA Patriot Act*, there is some concern that the definition of academic freedom may be narrowing (Altbach, 2001; Rajagopal, 2003; Association of University Professors, 2003). It has also been suggested that issues such as security and academic freedom ought to require an international focus (Altbach,

2001; Rajagopal, 2003; Rorty, 2003). Rajagopal (2003) argues that, in the absence of constitutional protections for foreign born faculty, researchers, and students, academic freedom might best be preserved by ensuring it as a human right. Bertrand Ramcharan (2004) points out that safeguards to protect human rights must be in place when protecting national security or countering terrorism as a country's human rights record is a crucial factor in assessing the level of risk.

Security and Freedom

One year after the 9/11 terrorist attacks, the American Association of University professors established the Special Committee on Academic Freedom and National Security in Time of Crisis. Resting on the premise that freedom of inquiry and the open exchange of ideas are crucial to national security, the report addresses government surveillance and intelligence gathering, free circulation of research results, electronic monitoring of foreign students through SEVIS, and suppression of political dissent and questions whether security and freedom are inescapably opposed (American Association, 2003). While researchers express concern over suppression and alteration of research results in university projects sponsored by private industry (Anderson, 2003; Healy, 2003; O'Neil, 2003), partnerships with government are also viewed as troublesome. Strict project management rules and the secrecy desired by DARPA (Defense Advanced Research Projects) and other military intelligence communities may inhibit scientific publication by academics conducting that research (Singer, 2001).

The Department of Homeland Security has promoted a policy of limiting scientific publication with a shift from a "right to know" to one of "need to know" in some

disciplines and the U.S. Department of Education has moved to eliminate links to researchers and organizations whose policies do not agree with those of the Bush administration (Tierney, 2003). Although there is a significant body of research on the benefits of cooperative research, policy debate has not included much about possible unintended consequences of these activities. It remains to be seen whether the decline in basic research and the chilling effect of secrecy resulting from university/industry cooperation will have a negative impact on the process of innovation (Behrens & Gray, 2001).

Technological innovation itself may have ramifications for course delivery and design as profit-making companies become involved in sponsoring cyber courses (Altbach, 2001) and universities develop intellectual property policies to share in the returns of knowledge production (Anderson, 2003). Along with the ability to create and disseminate digital copies of documents, music, film, and other media has come a shift in focus from the content of publications to one in which content and format are fused together. This has resulted in an alignment of publishers with technological innovators seeking stricter legislation to protect their common interests. As published works began to be considered in terms of format as well as content, publishers started lobbying for laws protecting their rights as property owners (Winant, 1999). Resulting legislation has included the *Digital Millennium Copyright Act* (DMCA), extending the time limits for copyright, and the *Uniform Computer Information Transactions Act* (UCITA), enacted in Virginia and Maryland, allowing for shrink-wrap or click-on licenses. In January 2003 the Supreme Court upheld the Sonny Bono *Copyright Term Extension Act* (CTEA) of 1998, which

extended the copyright term for new and existing works by twenty years (Birnhack, 2003; Eldred, 2003). While there is concern among scholars that this decision will reduce scholarly discourse about intellectual property issues, Samuelson (2003) suggests that, in light of the substantial consensus that CTEA is unconstitutional, future scholarship is likely to continue and may include new challenges to intellectual property rules. Etlin (1998) points out that, were education to be considered in terms of the public good, the intellectual capital rights of educators could challenge intellectual property rights. However, the private sector may also influence the structure of higher education institutions.

University/private sector relationships can be seen to influence the extent to which governance is shared in institutions of higher education as governing boards and administrators adopt corporate organizational models (Scott, 2002; Smith, 201). Pavleva (2001) describes academic freedom as a shared right which, as such, may lead to conflict. The way these conflicts are resolved will depend on public policy interpretations of the nature and aims of higher education. As university administrations look to the private sector in attempts to adapt to change and find ways to facilitate the speed with which decisions can be made, ideals of academic freedom such as free inquiry, open expression, discovery and dissent may be at risk (Scott, 2004).

While maintaining an open environment in academia is of concern to faculty researchers, openness is also viewed, more broadly, as necessary for supporting democracy (Feinberg, 2002; Tierney, 2003). Although public debate might help to engage the country in addressing important issues, there is concern that the Bush administration's framing of the current crisis as a war against terrorism has resulted in individual protections such as

free speech and privacy being conceptually transformed into opportunities for the enemy (Baker, 2003). As key information policy decisions are made by law enforcement and military personnel, it is possible that the move toward secrecy may become more pronounced. Interpretation of the *Freedom of Information Act* (FOIA) has traditionally been guided by the Justice Department and various Attorneys General who have used this power to both restrict access during the Reagan administration and to expand it during the Clinton administration (Feinberg, 2000; Halstuck & Chamberlin, 2001). In an October 2001 memo, Attorney General John Ashcroft, citing the safeguarding of national security and enhancing effectiveness of law enforcement, revised the standards by which the Justice Department defends agency decisions to withhold records making them more restrictive (Ashcroft, 2001; Feinberg, 2002). Legislation supporting non-disclosure in government is supported by private industry partners who have submitted cyber security or critical infrastructure and feel secrecy is necessary to induce private firms to cooperate with government (HB 2211, 2003; Peterson, 2002; Tien, 2001). The withholder of information may not necessarily gain an advantage by doing so, however, and might also be in danger of losing credibility (Keohane & Nye, 2002).

As the security of information about government and private industry becomes more difficult to access, concerns about security of information about individuals grow (O'Neil, 2001). Unlike copyright, there has been little debate about privacy within the context of networked information (Saksida, 1997). In their research on ISP (Internet Service Provider) contracts, Braman and Roberts (2003) found ISP agreements to disregard constitutional standards involving freedom of expression and privacy and

conclude that a significant shift is taking place, without public discussion or much public awareness. They suggest that public forum analysis could provide a legal foundation for seeking terms of service reflecting constitutional protections of civil liberties. Nehf (2003) argues that consideration of information privacy as a societal concern in a digital environment would allow the rhetoric of public debate to shift, thus allowing the range of politically acceptable policy solutions to expand. By providing a social structure focusing on the individual, rather than on an ideology, the Internet may prove an appropriate place for such a cyber political forum (Balkin, 2004; Galston, 2002; Jordan, 2001). Although culture has traditionally been produced though popular participation, the same features of the digital age that empower individuals also empower businesses. If this is so, it is possible that a conception of freedom of speech consistent with business interests may be inconsistent with the promotion of a democratic culture (Balkin, 2004).

A technological environment may have additional implications for public debate, as information security policy will determine both organization of and access to information being stored (Halstuk & Chamberlin, 2001: Westin, 1974). The *Electronic Freedom of Information Act*, signed into law by President Clinton in 1996 was designed to provide public access to records held by federal agencies and to ensure government accountability. This legislation grew out of concerns that a slow response to bridging the gap between technological development and laws related to freedom of information could restrict one's right to know (Halstuk & Chamberlin, 2001). After September 11, 2001 there was concern that public information available on the Internet could aid terrorists planning attacks on the United States. This concern led to both the policy statement by Attorney General Ashcroft

making it easier for agencies to deny requests for information and to an Internet content advisory issued by the FBI broadening the scope of information in need of restriction. In September 2002, Richard Clarke, the president's cyber security advisor, characterized the theme of the nation's cyber security plan as shifting to one of a "vulnerability paradigm" and outlined a strategy for closing security holes on the Internet (Vaida & Lawton, 2002). Federal agency response to these policy statements has included removing information from web-sites, establishing firewalls, limiting access, and discontinuing the updating of existing information.

As a goal of e-government was responsiveness to the public, it could be that the current policy of decreased disclosure could thwart the promise of e-government (Halchin, 2002; Tillman, 2002). Information policy resulting from these changes may also have an impact on the public's understanding of democracy (Feinberg, 2002). In the absence of access to information necessary to inform public debate, citizens could be left wondering whether threat scenarios are real or exaggerated (Naviakha, G., 1999; Rorty, 2002); and, perceiving greater risk, endorse more restrictive policies (Lerner, Gonzalez, Small & Fischoff, 2003). While policy questions may involve complexities that call for critical expertise in their formulation, policy in democratic polities ought not to be insensitive to democratically derived preferences (Dunn, 2003). When government or administrative expertise replaces citizen inclusion, it may devalue the authenticity of citizens by excluding them from public dialogue (Farmer, 2002).

A normative commitment to democracy may be a crucial factor in policy development after a terrorist attack. Dangers to the democratic state can come either in the

form of violence or in the loss of civil liberties, should the state's emergency responses be either too great in scope or too long in duration (Freeman, 2003). The Department of Homeland Security is the first federal agency required to include a privacy office whose mission is to minimize impact of security measures on individual privacy. Responsibilities for *Freedom of Information Act* oversight and for assessing impact of new technology on privacy have also been delegated to this office and the DHS Secretary and Chief Privacy Officer are both advised by the DHS Data Integrity, Privacy and Interoperability Committee on programmatic, policy, operational, administrative, and technological issues that affect individual privacy (U.S. Department of Homeland Security, n.d.) While privacy experts outside the federal government do credit the involvement of the DHS privacy office in the CAPPSII (Computer Assisted Passenger Prescreening System) project's reflecting more careful thought about citizen's rights, they still have concerns about government plans to use this information for criminal and immigration, as well as terrorist investigations. Although individual security measures may have become more respectful of people's privacy, the privacy office tends to remain faithful to the security agenda set by the department (Torobin, 2004).

The Inquiry

Information security policy may be seen as responding to an environment in which the roles of government, private industry, higher education, and non-profit interact in a variety of ways. At the same time, competing values such as public safety, civil liberties, private enterprise, and intellectual property may gain or lose prominence depending on how they are framed and presented to policy makers or to the public. This is all taking

place in an era when the pace of technological development exceeds the pace with which societal issues have historically been considered and policy developed. An approach to research into the context of information security policy development must be one that allows for complexity, can incorporate multiple perspectives, and will allow for a design to emerge based on what is revealed as important by participants in the research process. Research results, when studying a question like, "What is the meaning of security?" will not prove hypotheses and offer incontrovertible answers for all time. Rather, this is an honest attempt to assess what is important within this particular context at this particular time and offer a rich description to potential users of the research that may aid in understanding and expand their range of policy alternatives. In the chapter that follows I will outline the philosophical assumptions of the methodology I have chosen for this research and provide a detailed presentation of the methods used.

Chapter 3: The Use of Constructivist Methods for Interpretive Research

Determining the Appropriate Paradigm, Theory, and Methods

Complex relationships among government, private industry, universities, and others representing the interests of society emerge as information security policy issues decisions are made and policy developed to address diverse issues. Based on the literature review in the previous chapter, it seemed important to me to proceed with this research in a manner that would allow me to inquire into the idiographic and contextual understandings of the various stakeholders' perspectives and priorities, while asking the research question, "What is the meaning of security?" This inquiry has not sought to offer either objective descriptions of perspectives or relationships in this context. Rather, it represents the interplay of multiple meanings expressed as a result of the subjective experiences of participants in the study. Interest in the subjective role of participants' experiences, their insider perspectives, and the values that shape their understandings placed this inquiry outside the realm of traditional forms of inquiry and into an interpretive paradigm. As the goal of interpretive research is understanding, rather than description or generalization, it offers a paradigmatically distinct alternative to mainstream scientific methodology (Rodwell, 1998).

By attempting to understand the multiple meanings of security held by stakeholders in information security policy development, this inquiry provides a suitable research question for an interpretive paradigm. In this chapter, I present a theoretical perspective based on the writings of Richard Rorty and Martin Rein. In demonstrating the suitability of this theoretical framework for guiding my research, I discuss the focus, fit, and feasibility of the research question for constructivist inquiry as an appropriate interpretative alternative research methodology and conclude with elements of the research design that were utilized during the emergent process of the research.

Interpretive Paradigm Theory and Research

When adopting an alternative approach to inquiry, a researcher must discuss theory in a manner consistent with the paradigm. In the traditional research approach, taken in many dissertations, the role of theory is one that shapes assumptions and provides knowledge about the shape of the inquiry. In this respect, research helps to further develop or test theory (Creswell, 1994). Connections made between theory and research often include discussions of predictability, precision design, and methodology with the goal of generalization. These issues, related to theory development and testing, are not relevant to interpretive research, such as constructivist inquiry, where the emerging theory and knowledge should be grounded in the data. The focus of interpretive research is on the meaningfulness of findings for both the scholar and the user (Rodwell, 1998; Rodwell & Woody, 1994). While interpretive research does not rely on theory to determine the content of the study or the research design, an appropriate use for theory in this context

exists in its relation to the process of the research (Marshall & Rossman, 1999; Creswell, 1994).

The role of theory in this inquiry is not to provide justification for the content of the research and testing hypotheses. Rather, a theory of pragmatism is used in relation to the research process, supporting an emerging research design. This allows for inclusion of a hermeneutic process for discerning multiple meanings, idiographic understandings, and recognition of the role of values and context in the process of knowledge construction (Rodwell, 1998). As a researcher, I recognize that I have personal values, assumptions, and understandings of the topic and that, while theory is often used to frame a problem and help a researcher remain objective, in this intersubjective process of co-construction, my understandings are offered alongside those of other participants, so that theory relates less to what I know to be "true," and more to my process of knowing. Working hypotheses, along with criteria of rigor, presented in detail below, helped me to bound my subjective views, but in the mutual interaction of this shared inquirer/participant relationship, my assumptions did contribute to the knowledge being developed. Consistent with these and other assumptions of theory in an interpretive paradigm, the writings of Richard Rorty provide a framework supporting the subjective process of understanding multiple realities. The writings of Martin Rein support the grounding of theory and action in experience.

Rorty's Pragmatism

Rorty's pragmatism has its roots in the school of American pragmatism and the writings of Dewey, James, and Pierce. A philosophical approach to knowledge building that recognized ethics as a component in research methodology, American pragmatism

quickly became overshadowed by logical empiricism as the dominant theory for knowledge building. This pragmatic perspective argues against the relevance of eternal truths and seeks to define truth by its ability to solve a problem (Diesing, 1991). Richard Rorty's writings focus less on what is known to be true and more on what people experience as true. However, Rorty (1982) extends this theoretical position by emphasizing hermeneutics, a process through which perspectives are compared and evaluated, over epistemology, which values specific ways of knowing over others. Rorty's pragmatic theory of knowledge will help to articulate the assumptions of an interpretive paradigm and lead to a discussion of methodology that is relevant to the research question of this dissertation.

Rorty's work, rather than seeking to replace a dominant theory of knowledge, gives equal stature to many ways of knowing. Rejecting approaches to research based on the concept of objective reality, Rorty (1999) regards the purpose of inquiry to be agreement among human beings on a course of action. *Solidarity*, or the pragmatic purpose of cooperative human inquiry, from Rorty's perspective, is the purpose of inquiry, as opposed to the ability to generalize about universal truths (Rorty, 1989; 1991, 1999). Not limiting himself to any disciplinary framework, Rorty (1999; 2002) recognizes the importance of freedom and openness in reaching consensus on workable solutions and favors intersubjective interpretations of experiences, as pragmatic understandings promote hope and allow for improving the future as a goal for research.

Rorty (1991) acknowledges the importance of context by asserting that the starting place for the researcher must be with the assumptions, beliefs, and perspectives he finds.

At the same time, *irony*, or the understanding that the way something is understood in one context or at one time may be different from how it is understood in some other set of circumstances, allows Rorty (1998) to focus on justification of beliefs, rather than proving their universal truth recognizing that there may be competing understandings of truth. In doing so, the research emphasis becomes a creative one and research participants play an active role in shaping those understandings in ways that contribute to sense making. Recognizing that the usefulness of an idea cannot always be known in advance, Rorty (2002) values the importance of the imagination in extending the notion of what might be useful.

Rein's Action Framework

Martin Rein's work focuses on translating theory into practice. From Rein's perspective, knowledge and action are reciprocally connected. Rather than assuming that thought always precedes action, he sees both as being shaped by interests arising from existing institutions and programs that exist within a context. Asserting that knowledge of fact and commitment to values both arise from the realm of action, policy research must start with a commitment to action and actors (Rein, 1983). At the same time, framing is necessary for making problematic situations comprehensible. Rein (1976) offers the context for use as a value framework within which to consider multiple perspectives and differing courses of action (Farmer, 2000). By using the framework in this way, policy makers are offered the opportunity to temporarily adopt a particular point of view. This allows both for the ability to move among a number of policy choices without, necessarily, committing to any of them and the conceptual space needed for creativity (Farmer, 2002).

For Rein (1976), the search for a perspective from which to analyze policy can be limiting, in that it tends to separate those aspects of policy analysis that work together in policy development. "Policies are in fact interdependent systems of: (1) the abstract values we cherish; (2) the operating principles which give these values form in specific programmes and institutional arrangements; (3) the outcomes of these programmes which enable us to contrast ideals and reality; (4) the often weak linkages among aims, means and outcomes; and (5) the feasible strategies of change this pattern suggests. Few studies of policy attempt to draw these themes together" (Rein, 1976, p. 141). For a constructivist inquiry, however, it is essential for multiple realities to be of interest and for the problem being investigated to be one with many constructions (Rodwell, 1998).

The Constructivist Inquiry

Throughout my research, I considered the multiple truths that were shaped by beliefs and values held within the context of the inquiry, seeking better understanding, rather than universal truth, and considering my own perspective in the same light as those of all other participants. In the course of this inquiry, I expected to encounter those who believed that issues of national security outweighed individual privacy concerns, those who believed that individual freedoms were paramount, and those who viewed information policy concerns as secondary to concerns of the market. I also anticipated speaking with some who viewed technology as a tool with which they could respond to security issues and others who viewed technology as opening up a whole range of new security issues to be dealt with. My aim, however, was not settling on a particular view to adopt, but on assuring that multiple perspectives were honestly considered and portrayed and that there

was an accurate construction of the diverse understandings of the relationships among security, technology, and policy-making. While my goal was to improve my own understanding and the understandings of others, I also remained hopeful that this understanding would be of practical use to policy-makers and others who make use of the study.

Focus, Fit, and Feasibility of the Research

These goals and the theoretical and paradigmatic assumptions, the research question found an appropriate focus and fit in the constructivist inquiry and was also feasible to implement. I will discuss my decision to use constructivist methods by answering questions related to the focus, fit, and feasibility of the research. These considerations helped to determine if constructivist inquiry was able to offer a methodology appropriate to the emerging questions related to the issues surrounding information security policy development.

Focus. One of the unique features of constructivist inquiry is that it can be employed in pure research, evaluation, or policy analysis and allows for a combining of these three traditional types of research as the study evolves (Rodwell, 1998). To the extent that I proposed to study the meaning of security within the context of public policy, the focus of this dissertation was determined to be pure research. As pure research, I sought to explore varying perspectives and values of policy makers, technologists, and other stakeholders in information security policy development. I anticipated, however, that while this inquiry began as pure research into these groups' understanding of the meanings of security, technology, and the interplay of the two, policy implications might emerge, as

information security policy and legislation contribute to the multiple understandings of the phenomenon.

As a qualitative methodology, constructivism is concerned with process and meaning, not cause and effect (Bogdan & Biklen, 1998). It is helpful to consider the processes by which constructivist research inquires into the purpose and values of policies (policy-in-intent), issues of policy and program effectiveness (policy-in-implementation), and experiences of policy results (policy-in-experience) (Guba, 1985). All of these aspects of policy analysis did emerge in the course of this research. Elements of policy-in-intent were evidenced as participants spoke about policy ideology incorporating non-disclosure or secrecy for purposes of information security, and recognized that there are features of non-disclosure that appear to make security less effective than full disclosure or a policy of openness. Features of policy-in-implementation were observed in discussions of policies designed to protect data that lacked sufficient components for assuring the quality of already existing data; and aspects of policy-in-experience were revealed in participants' discussions about experiencing the loss of civil liberties as a result of policies designed to enhance their security. While these policy implications emerged during the research process and are discussed in chapter five, the focus remained phenomenological and, as such, was conducted as a process of pure research.

Fit. Constructivism requires that the assumptions that undergird the research question fit with the assumptions of the interpretive paradigm. As multiple perspectives or realities are of interest and interaction between the inquirer, the phenomena to be investigated, and the context is important for understanding (Rodwell, 1998), my research

question, exploring the meaning of security, fit well with these assumptions. Multiple realities were expected, as numerous participants responded to questions about the meaning of security and based their responses on differing assumptions, values, and definitions.

Subjective interaction of individual meanings is also central to this inquiry. Data collected through interviews represented multiple views of participants, including my own. By engaging in a hermeneutic process that allowed for insights to be shared, tested, and evaluated, perspectives were placed in contradiction, thus allowing for a higher level of understanding (Rodwell, 1998). This hermeneutic dialectic was assured by promoting interaction among participants and conducting member checking, in which participants verified recorded data, to assure the accuracy of the various representations of reality.

Assumptions that only time and context-bound idiographic statements are possible for understanding are central to constructivism (Rodwell, 1998). Therefore the parameters of the study in which working hypotheses are developed must be clear and results considered in light of frameworks that are bound by context. The aim of this inquiry is not to generalize to another setting, but to provide a rich and accurate reconstruction of various perspectives within the particular context of the research and the following working hypotheses were developed based on these assumptions:

- *H1*: Policy makers rely on technological experts in the development of information security policies.
- *H2*: Policy makers and technological experts often use different terminology.
- *H3*: Values underlying assumptions for these two groups are different.

While these assumptions remained a basis for the research design, as it developed, and throughout the course of the inquiry, changes in the interview protocol and the expanding range of participants demonstrate the emergence of a design reflecting the increasing complexity I found in the environment under investigation.

The context of this research was bound by responses to information security issues from participants in the sites studied and began with policy makers and technologists within state agencies in the Commonwealth of Virginia. As Virginia state agencies have all been required to develop information security plans, I expected answers to my initial interview questions to include responses related to development of policies in response to these directives. Doing this allowed me to then begin the hermeneutic process by taking these responses forward for others to react to and by revising my interview protocol, as participants provided direction to the research process. This hermeneutic process contributed to an emerging design that was guided by participant responses both in terms of content and inclusion of future participants, as each person was asked to recommend others with the understanding that I was seeking the widest possible range of perspectives and to provide me with names of prospective participants with viewpoints other than their own. These multiple perspectives, including my own, provided the data from which theory emerged.

The theory produced through this co-construction of meaning in this inquiry is one in which the government, university, private sector, and non-profit sectors might best be described as existing in a symbiotic relationship. While each entity is recognized as having its own unique power, the complex network of interactions observable in the

research demonstrate communications of a subjective and intersubjective nature among these groups, as well as those representing concrete action and policies and procedures. By according status to all of these, policy makers can remain open to and gain from the complexity as they develop policy in an unstable environment. This emergent theory is discussed in more detail in chapters four and five.

Lincoln (1985) and Guba (1985) suggest that complexity of joint action in the areas of policy analysis and public administration, along with the impossibility of anticipating consequences, may be significant elements in a paradigm shift within the policy sciences to a macro-organizational approach that recognizes horizontal, as well as vertical relationships. Rodwell (1999) offers criteria for a problem suitable for constructivist inquiry. Values must be central to the problem and it must be sufficiently complex to warrant this kind of investigation. Along with the wide range of values that I encountered while studying information security policy development in this context, my own views, as a librarian adhering to a code of ethics emphasizing the importance of privacy rights, academic freedom, and access to information have played some part in shaping the construction of meaning in this study and were included with the those of participants from a number of disciplines, ideologies, and experiences, representing a wide spectrum of values.

Feasibility. The research was determined to be feasible as demonstrated by the access that I had to a variety of participants needed for the inclusion of multiple perspectives and the low level of risk inherent in this research process. Administrative colleagues in the Virginia Community College system helped me obtain access to

participants in the governor's cabinet and newly formed security institutes in Virginia. Through these participants, I was able to obtain access to the wide range of perspectives needed, including those of participants in federal government, university policy institutes, international think tanks, and private industry. As a public administrator in higher education, my prior knowledge of the setting was helpful in allowing me the flexibility and adaptability necessary at the beginning stages of the inquiry (Rodwell, 1998) and helped me to obtain the maximum variation necessary to ensure the richness of the study. While this study revealed vast differences in views among participants, its aim of exploring the multiple meanings of security was not one that was likely to put participants at risk or be perceived as particularly threatening, as policy makers, technologists, and other stakeholders clearly expressed the opinions that shape their realities. Moreover, the timeliness of the topic of security research was often attractive to participants who were also interested in gaining knowledge in this area. At the same time, it was important to remain cognizant that, in an area where discourses may be competing, the researcher's attention to being perceived as neutral and non-judgmental was extremely important. "Though the researcher positions himself or herself on the same plane of understanding as those who participate in the process, there must be another level of the researcher's conscious use of self (in the practice sense) that assures the use of the appropriate tool or role to carry out successfully the hermeneutic process as the process emerges" (Rodwell, 1998, p.86).

Another important consideration was making sure that asking questions about security did not put participants on guard against revealing too much or violating security.

I approached the interviews in such a way that it was clear that I was only interested in what participants had to tell me and I reassured them that they would have the opportunity to take part in a member checking process. If the value of the hermeneutic circle is in its ability to promote understanding by getting below the surface (Farmer, 1995), both interviewer and interviewee must be comfortable to effectively search for mutually shared meaning (Rodwell, 1998).

Constructivist Methodology for Exploring the Meaning of Security

Constructivist inquiry provides a method of interpretive research that allows for multiple meanings of security and, at the same time, recognizes that these subjective understandings are based on peoples' experiences and the context in which they take place. Constructivist methods attend to the knowledge building process, while allowing for emergence based on the construction of participants' meanings and changes in these meanings. Constructivist methodology has three distinct phases to which I attended. However, as the emergent nature of this research design was based on the experiential process of my interaction with the participants, exact content of each phase could not be known in advance, but is discussed as the design emerges.

Phase I: Orientation and Overview

Initial Bounding of the Problem. The first step is a description of the problem and context that usually emerges from the prior knowledge of the researcher or a review of the literature about what is important for understanding (Rodwell, 1998). My initial interest in the meaning of security came out of a realization that various participants involved in the policy-making process seemed to be using different kinds of language or different

definitions as they discussed issues of information security and technology. A review of the literature confirmed that both security and technology are often studied in isolation of any societal impact and that definitions of these terms are not consistent. Moreover, while policy-makers often rely on advisers and technical experts in making decisions, it seemed that, depending on who was framing this information for decision-making, the policy outcomes could be very different.

In constructivism, prior ethnography refers to a method for gleaning information about values, culture, and human and political structures in order to bound a context (Rodwell, 1998). My foreshadowed questions for use in data collection were shaped by both a review of the literature and a prior ethnography among stakeholders in security and information policy decision making in higher education and related entities. Foreshadowed questions included:

- What are the priorities of those engaged in discourse surrounding information security policy?
- What is the meaning of security?
- What is the meaning of technology?
- What role does framing play in problem definition?
- Who is doing the framing?

These foreshadowed questions formed the basis for my interview protocol, which initially allowed me to become better informed about the topic under investigation. The interview protocol was revised three more time. These revisions were, at first, based on efforts to clarify responses and eliminate repetition:

- Please talk about technological language in policy writing.

- In your opinion, what are the important security issues for colleges and universities?

Later changes allowed me to incorporate initial responses for others to react to and contributed to a more sophisticated understanding of the shades of difference in meaning exhibited by the participants. The final version of the interview protocol consisted of the following questions:

- It appears that the word *security* may be defined and used differently in different contexts. How would you describe the concept of security and what do you mean when you talk about *security*?

- The word *technology* also seems to be defined in a variety of ways. What do you mean when you talk about *technology*?

- How do you think of technology in relation to security?

- From your perspective, what are the important information security issues for colleges and universities?

- Who do you see as the stakeholders in information security policy development?

- It has been suggested that framing plays a part in policy development. Would you comment on this?

- It has been suggested that there is a language that goes along with technology. What do you think about this?

- There appear to be conflicting views on the use of technological language in policy writing. Would you comment on this?

Natural Setting. Constructivism requires that research take place in a natural setting and that the researcher be able to interact with the setting and its inhabitants (Rodwell, 1998). In order to develop foreshadowed questions to guide the research, prior ethnography, or the process of combining prior knowledge with the phenomena being

investigated, must take place. Prior ethnography contributes to the researcher's ability to interact with and to understand participants and their constructions of reality. Context is central to constructivist research, as a phenomenon can only be understood within the setting in which it is observed. Because of the interactive nature of the inquirer/ participant relationship, the ability to relate in some form of consensual language is necessary for knowledge building (Rodwell, 1998).

This research involved policy makers and technologists at the university and other levels within a bureaucratic context, as they both responded to and influenced public policy with regard to security. As the researcher, my familiarity with and tacit knowledge of the context, along with a variety of multiple perspectives of those involved in discussions about information security policy, allowed for relative ease of entry into the research and contributed to making this an appropriate setting for a constructivist inquiry. Interviewing took place in the workplace of each participant, whenever possible. In doing this, I sought to enrich the process by making an effort to recognize and include elements of the setting relevant to this research. This process consisted of examining records and documents in addition to my observations recorded in the field notes. Aside from contributing to understanding of issues related to the research, this approach provided a background for the development of additional, pertinent research questions and allowed for triangulation, or the process of using several modes of data collection to support and verify data collected and analyzed (Rodwell, 1998).

Criteria for Rigor. In constructivist research, rigor involves the demonstration of trustworthiness, authenticity, negotiated outcomes, and maintenance of the quality of the

hermeneutic circle (Rodwell, 1998). A process for assuring these components was maintained beginning in the first phase by setting up processes for reflexivity, peer review, and methodological decisions. This was done through the maintenance of reflexive, methodological, and peer review journals, as well as making arrangements for a qualified peer reviewer to accompany me throughout the process and an auditor, schooled in constructivist methods, to conduct a trustworthiness and authenticity audit of the final case report. Reflexivity, which involves awareness of one's knowing processes, is valued in constructivist inquiry as it allows the researcher to be attentive to use of self and the role of emotions, values, and reactions (Rodwell, 1998). I maintained a reflexive journal that includes thoughts, feelings, values, and beliefs relevant to emerging issues and problems related to research in information security policy development (Lincoln & Guba, 1985). Methodological decisions related to the emerging design were maintained in a similar form through use of a methodological journal (Lincoln & Guba, 1985) and a peer review journal chronicled my interaction with a peer reviewer. These tools facilitated mindfulness of the process in ways that encouraged trustworthiness and authenticity.

Peer Debriefing. In constructivism, a peer reviewer accompanies the research process, posing searching questions to help the researcher better understand his or her own perspective and behavior throughout the course of the research, and to test working hypotheses outside the inquiry context, thus enhancing the emergent design (Rodwell, 1998). While peer debriefing is primarily utilized during Phase II, my process of orientation and overview included making arrangements for it to take place. Dr. Pamela Kovacs, an associate professor in Virginia Commonwealth University's School of Social

Work, has served as primary peer reviewer for this study. Dr. Kovacs has studied constructivism and other qualitative methodologies and teaches M*ultiparadigmatic Qualitative Methods and Analysis* at VCU. I previously served as an auditor for a constructivist project of Dr. Kovacs' and knew her to have the technical ability and expertise required for her role as peer reviewer (Rodwell, 1998). In addition, I regularly met with a group of colleagues knowledgeable in constructivist methods and inquiry and these ongoing conversations have contributed to both critical thinking and attentiveness to ethical and methodological issues (Rodwell, 1998).

Ethical Considerations. Research ethics call for minimizing risks to participation and assuring that participants are informed in their consent to be part of the research process (See Appendix C for a Research Subject Information and Consent Form). There are also degrees of confidentiality for participants that should be considered in constructivist inquiry (Rodwell, 1998). The process of meaning construction, including the development of knowledge in what will be described below as a hermeneutic circle, suggests that it may be possible for participants to identify each other. While identifying information, such as names of participants, were not used in this research, it may be possible to determine participants' organizational context, meaning that strict confidentiality cannot be assured. I have tried to protect the identity of participants throughout this process. Accordingly, steps were taken to help ensure that identity could not be determined through conversational detail. These considerations were discussed with participants and were available to them in the Research Subject Information and

Consent Form that they signed and which met the requirements of the Virginia Commonwealth University Institutional Review Board.

Phase II: Focused Exploration

In moving from the phase of orientation and overview, it is important to recognize that the second phase of exploration emerges from the earlier elements of the research experience. The second phase of the constructivist inquiry is the actual focused exploration into the multiple perspectives surrounding information security policy development.

Sampling. In constructivism, sampling should be purposeful in order to allow for the evolving nature of the design (Rodwell, 1998). Uniqueness of the particular phenomenon for observation can best be understood by paying close attention to the diversity within the sample and maintaining maximum variation as a goal in sampling, as the typical case can help provide a sense of what is normal in a context and the outlier can be useful in providing new insights (Patton, 1990; Rodwell, 1998). In this study, a purposive sample included the widest possible range of stakeholders in the arena of information security policy development. Stakeholder groups emerged from the initial groups identified during the research process to, ultimately, include participants from state and federal government, private industry, and the non-profit sector who were each identified as having a significant role by other participants. At the point where new participant categories ceased to emerge, referrals became repetitive, and new data began to duplicate what had been collected, I concluded that seeking further categories and candidates would not add significantly to the study and could make data analysis

cumbersome, as well as result in diluting the inquiry. It was here that I determined I had reached the point of redundancy (Patton, 1990).

Because of the non-threatening nature of this inquiry, in which I would meet with participants in the context of their organizational roles in their work environments, a need for beginning with gatekeepers was not required. However, in the sense that some participants were very difficult to access and had to sometimes be approached several times through other different participants, the process of beginning with contacts known to me and branching out led to some participants assuming the role of gatekeeper at certain times during the research process. Beginning with policy makers and technologists in higher education and state government, I remained open to the possibility of new stakeholders and participants were continually nominated throughout the course of the research, which both assured emergence and the bounding of the process. This sampling method in which participants are asked to nominate other stakeholders whose views and values may differ from their own has been described as snowball sampling (McCall & Simmons, 1969).

The emergent sample of multiple stakeholders within the context included participants who exhibited a wide range of perspectives, priorities, and understandings of the relationships of the interplay of security and technology and the roles that it plays in developing information security policy, as well as multiple meanings of the ways in which the various actors influenced policy and each other. Twenty-five participants from twenty different organizations participated. Figure 1 illustrates categories by organizing them within a chart using my beginning definitions. While this chart is meant to give a clearer

picture of the context, it cannot adequately reflect the relationships or interconnected nature of the groups or individuals in question. For example, as some colleges were state supported, participants in those sites could have also been included in the state government column. Also, there were clearly participants who worked in technology and, while considered technologists for the purposes of the chart, also developed policy and could have been put into the category for policy makers. I use these examples, but other ways for these participants to interact also exist. With this caveat, however, I believe this figure to be useful in demonstrating where the research led.

Participant Category	**College/ University**	**State Government**	**Federal Government**	**Private Sector**	**Non-profit Sector**
Policy Makers	6	1	3		1
Technologists	7	3		1	1
Other				1	1

Figure 1. Participant and Site Categories

With the understanding that some categories of participants were more clear cut than others, the categories represented above are defined in the following ways. The policy making group included individuals with responsibility for developing information security policy. This included, but was not limited to elements involved in protection of data, records, networks, identifying information of individuals, privacy, copyright, critical infrastructure. Technologists were identified as those with specific responsibilities for technical aspects of networks, systems, hardware, software, and other technical aspects that can be considered elements in the aspects of information security policy development listed above. In addition, in the course of the research, I was led to the private sector when public/ private sector partnerships and related interests in critical infrastructure protection,

among other issues, highlighted the importance of this group for the study. Likewise, as other organizations do influence policy and participants from those sectors had related interests in civil liberties and other issues, the non-profit sector also bounded this investigation. The case study in the next chapter will provide more detail and a more accurate portrayal of the interaction of these participants and groups within the context just described.

Use of the Human Instrument. In the research process, the inquirer became the primary data collection instrument (Rodwell, 1998). This allowed for adaptability in recognizing, sorting, and respecting a plurality of meanings. Unstructured interviews were conducted to collect data because of the flexibility and responsiveness they allow for the human instrument. Having studied qualitative research methods, including those specific to constructivism and employed in this study, and participated in qualitative research interviews, I understood the importance of remaining attentive to personal and contextual cues that can provide meaning. In addition, my tacit knowledge allowed for maneuverability within the research context.

Qualitative Methods. Face-to-face interviewing in the natural setting of the participant allows the complexity of the topic to be explored and understood from that participant's own frame of reference, as both the purpose and the context contribute to what is actually being said (Bogdan & Biklen, 1998; Rodwell, 1998). In this way, the qualitative methods of in-depth interviewing and participant observation are employed simultaneously. During this process I, as the researcher, took field notes and extended field notes including data from both interviews and observation. Immediately after each

interview, extended field notes were entered into Microsoft Word with a numbered-line format to prepare data for analysis and to aid in the reconstruction of data necessary for an audit (Schwandt & Halpern, 1988). In addition, I recorded my personal reactions or analyses in my reflexive journal, which helped me to chronicle the steps in the process and assure logical progression in the development of my methodological journal (Rodwell, 1998).

The goal of the inquiry, for the purposes of co-construction, is to be able to recast tacit knowledge into propositional form as soon as possible after data are collected (Rodwell, 1998). As constructivism relies on the tacit knowledge and sensemaking of interactions that can only be provided by use of a human instrument, no tape recording was used. The researcher and the participant are both present in the context in which interaction must be evaluated, bias identified, and meaning constructed. "It would be virtually impossible to devise a priori a nonhuman instrument with sufficient adaptability to encompass and adjust to the variety of realities that will be encountered" (Lincoln & Guba, 1985, p.39).

Hermeneutic Circle. A hermeneutic circle of information, in which the inquirer facilitates the sharing and testing of information from a wide range of stakeholders, was employed in this study. My purposive sampling plan called for me to elicit the names of additional participants from those already participating in the study, whose views were different from their own. When these participants discussed differences in perspective, the contrasting perspectives often led to increasingly greater understanding, which demonstrated the dialectic nature of the hermeneutic process. This is evident in the case

study that follows. While there was potential for conflict in the ways priorities were set for participants with varying perspectives, the topic and the nature of the study were not threatening nor did they inhibit honest communication. I made a point of informing participants of the details of the process and its emergent nature. In addition, by making sure that they were assured of confidentiality and knew that I would make every effort to accurately record their voices, participants were encouraged to participate honestly and seemed to be comfortable with the process. By engaging in the hermeneutic process, I attempted to demonstrate respect for all points of view. Member checks assured this by allowing participants to react to the extended field notes and case report and by these reactions being noted in my journal.

A hermeneutic circle is a circular process of information sharing that allows for the development of meaning utilizing and building on data from interviews, documents, literature, observation, working hypotheses, and other sources. In my role as researcher, I have been responsible for this cycling of information that shapes the construction of meanings related to the research question. This has meant acting as both teacher and learner in the co-construction of meanings by taking information from one interview to the next and back again. I have had to continually see myself as a collaborator in order to assure a quality hermeneutic process of mutual understanding and a quality co-constructed product (Rodwell, 1998). Quality of the hermeneutic circle was maintained through the use of ongoing member checks, as participants confirmed or revised transcripts I'd constructed from my field notes.

Inductive Data Analysis. In inductive data analysis, the direction of the research only becomes clear after the data have been collected. Theory emerges as a result of constant comparison of data recorded in the field notes, moving from specific data to general themes (Glaser & Straus, 1967). Then, in the unfolding of the design within the context, the results of data analysis emerge (Rodwell, 1998). In constructivism, this process takes place through the activities of unitizing and categorizing. Unitizing involves the identification of units or the smallest pieces of information capable of being understood by those with minimal knowledge or experience of the phenomenon under investigation (Rodwell, 1998). Units are arrived at by deconstructing the field notes. As each unit was identified, it was transcribed onto an index card and coded so that it could be traced back to its original source and context. A total number of 1,179 units were identified for coding. I employed a coding scheme that identified which participant the unit should be associated with, the respondent type, the interview number, and the unit number. As I made decisions about coding, I entered them into my methodological journal.

Categorizing took place after all units had been identified. This was done through *sorting*, or organizing index cards by theme and by *lumping*, which brought units with similar themes into provisional categories (Lincoln & Guba, 1985; Rodwell, 1998). After the sorting occurred, units were lumped into broad or over-arching categories, for which category labels were defined. Through this process, a rationale or decision rule was provided for determining the assignment of specific units to a particular category. Categories were then further subdivided. This continued until all possible relationships were found between abstract categories (Rodwell, 1998). During this phase of the

analysis, I continued to consider relationships between categories, as well as further divisions until I arrived at meaningful categories and sub-categories that accurately represented the themes identified. This process resulted in the development of four major categories with multiple sub-categories from which the grounded theory of meaning has been constructed in the case study. Category sets with decision rules and codes can be found in Appendix D.

Phase III: Comprehensive Member Check

Case Report. Phase three in the research process consists of the completion of the case report, a final member check with participants to negotiate meaning, and an independent audit of the report. A report on the multiple meanings of security expressed by policy-makers, technologists, and other stakeholders joining in discourse surrounding information security policy development provided a thick description of the research process and results of the co-construction engaged in by the participants in the inquiry. The report contained all data collected in order to assure the inclusion of all perspectives. In addition, assertions made in the report were grounded in and linked back to the raw data for use in the audit process. The case report was written from an emic perspective, in that my role was that of an insider, and demonstrated an understanding of the complexity of the concepts involved in negotiating meanings of security. The report is context-bound and no attempts were made to generalize results to any other context. Rather, an idiographic interpretation focused on the uniqueness of the report to the context of the inquiry (Rodwell, 1998). In addition to including participants representing maximum variation, efforts were made to assure that all viewpoints, including any that departed from any

consensus, were included. It is through the recycling of minority results for further consideration within the hermeneutic process that the inquiry comes full circle in the process of co-construction (Rodwell, 1998).

Meaning emerges through the data analysis and the construction of meaning through defining categories and sub-categories. A case report that provides a sufficient basis for understanding the context being studied results in a thick description that may aid in transferability (Lincoln & Guba, 1985). What is important in a constructivist inquiry is not the ability to generalize to other settings, but to use thick description to produce a case study report that richly and accurately represents the range of perspectives within the context of the investigation. It is the informed reader of this report, then, who may determine its relevance in some other settings (Rodwell, 1998).

Negotiated Outcomes. Participants in the study attested to the accuracy of the re-construction by identifying their own voices in the report by means of a final member check. This member check constitutes a major component of constructivist rigor, as it demonstrates both the trustworthiness and authenticity of the study. Five of the twenty-five participants interviewed were selected to read the case report, find their own voices, comment on how their perspectives were portrayed, and suggest revisions. These selected participants represented: a small community college, a large university, a state technology agency, an international think tank, and private industry. As ongoing member checks had taken place throughout the course of the research and I had made every effort to present an accurate picture of the context in the case report, I did not expect major revisions. This final member check resulted in a confirmation of the case report and no further revisions.

Criteria of Rigor

While constructivism focuses on the relevance of the research, assuring quality throughout the process is also important to the inquiry (Erlandson, Harris, Skipper & Allen, 1993). Trustworthiness and authenticity are two sets of criteria for rigor in constructivist inquiry (Lincoln & Guba, 1985). Trustworthiness is largely analogous to issues of reliability and validity in traditional research paradigms and focuses on credibility, transferability, dependability, and conformability (Lincoln & Guba, 1985; Rodwell, 1998; Schwandt & Halpern, 1988). Authenticity, established with particular relevance to assumptions of constructivism, focuses on the interactive quality of the inquiry process (Guba & Lincoln, 1989; Rodwell, 1998).

Trustworthiness. To assure quality of the inquiry and resulting report, four criteria were utilized to establish and assess trustworthiness (Rodwell, 1998). *Credibility* seeks to assure that research findings accurately reflect participants' constructions of meaning. Time and resources utilized during this inquiry were sufficient for prolonged engagement and persistent observation assuring a fullness of depth in data collection, a level of trust between inquirer and participants, and a depth of understanding of the multiple realities being constructed. A methodological journal and reflexive journal were used to record results of triangulation. Peer debriefing included the asking of critical questions regarding the accurate reflection of participants' meanings. Journal notes from peer reviewers were available during the audit to reflect this process related to credibility. Member checks took place and were documented throughout the process and with the final report, as I sought

reactions from participants. The audit report serves to confirm the accuracy of meaning as it was used in the case study and as it was reviewed in the credibility audit.

Dependability is determined in the final audit and assures that emergent decisions made in relation to the research design and methodology are documented and are congruent with constructivist standards. A methodological journal and peer debriefing were used to record and justify these changes as they occurred in the inquiry process. The measure of *confirmability* demonstrates that the research results are linked to the data collected in the inquiry. This involves tracing of information in the case report back to the transcripts through the data units. Triangulation and member checking support confirmability and the audit allows data reconstruction to assess both of these elements of trustworthiness.

The reader of the report helps to determine levels of *transferability*, the final element of trustworthiness. If, in the process of reading the case study, a reader is able to determine relevance for another context, transferability has occurred. This is best accomplished through a thick report (Zeller, 1987). This thick description in the case report offers an entry for the reader into the research experience and an appreciation for information grounded in the context (Bouma & Atkinson, 1995; Lincoln & Guba, 1985; Rodwell, 1998). While transferability is not the primary goal in a context-dependent inquiry, it is up to the reader to determine the value and usefulness of the report. The responsibility of the author of a constructivist case report is to use this report as a vehicle to convey meaning to potential users of the research. By using a method of reporting that highlights the interplay between the participants and the researcher/participant and allows

the reader to probe for internal consistency, the research remains congruent with the requirements of constructivism calling for rigor in terms of trustworthiness and authenticity (Lincoln & Guba, 1985; Rodwell, 1998).

Authenticity. Authenticity is a criterion of rigor unique to constructivism and has been considered throughout the inquiry process. This criterion, attending to the quality and integrity of the process, has been achieved through the recognition of five dimensions of authenticity: fairness, ontological authenticity, educative authenticity, catalytic authenticity, and tactical authenticity. These dimensions of authenticity were discussed with participants at various phases of the inquiry. It is in a consideration of authenticity that the research maintains rigor as well as relevance, and promotes ethical and reciprocal interaction among the researcher and participants. The authentic quality of this inquiry can be judged by the extent to which participants have: an even-handed representation of all views (fairness); increased awareness of the complexity of their experiences and the social environment (ontological authenticity); increased understanding of and respect for the constructions of others and their impact on other participants (educative authenticity); a changed situation or a changed experience within the context (catalytic authenticity); a redistribution of power among the participants and stakeholders in the process to act or bring about change (tactical authenticity) (Guba & Lincoln, 1989; Rodwell & Woody, 1994).

Measures to assure fairness throughout the research process included ongoing member checks, where every participant had the opportunity to read transcripts derived from my field notes of their interviews and make revisions. Throughout this process,

participants acknowledged fairness in the process as they demonstrated an appreciation for the issues under consideration and expressed their diverse perspectives. The author's even-handedness in the representation of views in the case report is an aspect of fairness that is dealt with in the audit, as the auditor must be able to find links to all of the data collected. In consideration of ontological authenticity, participants made comments about realizing that there are many views and acknowledging complexity of the context. They were able to recognize multiple meanings and, to a certain extent, develop an understanding of the differences in perspective. Participants recognized the roles that others' perspectives play in policy development and this process of understanding encouraged respect for alternative views, demonstrating educative authenticity.

In a research environment that is interactive and allows for the expression of multiple perspectives, it was possible that participants' views might have been altered by exposure to new information or new ways of thinking about the concept of security and all that it encompasses. Heightened awareness and a more sophisticated understanding of the world can be natural outcomes of a constructivist inquiry (Rodwell, 1998). By recognizing other perspectives and engaging in discussions that allowed for their inclusion, a more sophisticated approach to policy development may result. A concentration on organizational variables to the exclusion of the interconnectedness of members' roles, can result in an unprofitable narrowing of the range of consideration of organizational lives (Guba, 1985). Whether or not this heightened awareness actually results in different policies, it may extend the range of acceptable policies (Rein, 1976).

As those involved in the study commented about the interview questions causing them to think about things they hadn't before or putting things in a new perspective, they exhibited catalytic authenticity. One technologist who participated in the final member check spoke of having spent his entire professional life under the assumption that trade-offs between security and access were necessary and added that, while not being totally convinced, he was intrigued by the notion that there were other ways of thinking about this. While I did not witness the redistribution of power that comes with tactical authenticity, it is possible that this could occur as a result of transferability after reading the case study.

Audit. The audit process is relevant to research rigor as it allows an outside source to examine the process of data collection and analysis. Kate Didden, a Ph.D. candidate in Virginia Commonwealth University's School of Social Work, conducted the audit for this inquiry. She has completed a course in constructivist research and is currently conducting her own constructivist dissertation research. Her audit responsibility included examining the process that I have conducted in an attempt to verify the quality and rigor of the inquiry. She assessed methodological processes, the data collected, and the analysis of the data leading to meaning construction in the case study report in a Trustworthiness and Authenticity Audit. This formal examination of the details of the research process and product assured that the level of rigor used throughout the inquiry was appropriate and that the product reflects the process (Rodwell, 1998). The auditor's report is included as Appendix F.

Chapter 4: Interpretations

Introduction to the Case Study Report

In the previous chapters, I have attempted to lay the groundwork for research exploring the context in which information security policy is developed as well as provide a rationale for employing a naturalistic research model and a constructivist methodology as an appropriate way to conduct this inquiry. In an environment where a number of definitions for terms such as *security* and *technology* are used simultaneously and information is framed and presented to policy makers by persons with varying priorities, values, and agendas, it seems clear that what is important for the reader's understanding in interpreting this research report is, to the greatest degree possible, to become immersed in the context. It is through thick description in the case report that a reader is offered a window into the research experience and best able to appreciate information that is grounded in that context (Bouma & Atkinson, 1995; Lincoln & Guba, 1985; Rodwell, 1998). Further, it is through the style of the case report that the researcher can send a message as to what is to be considered legitimate epistemology (Zeller, 1999).

When employing a naturalistic research model, the constructivist researcher interacts with participants in the research context and they can be said to influence each other (Erlandson, et al, 1993; Levison, 1974; Lincoln & Guba, 1985; Rodwell, 1998). The language of the researcher, then, not only contributes to meaning within the context, but

also in conveying that meaning to those who would make use of the research. Rather than defining language as a tool for mirroring the object world, it is viewed here as inseparable from human intention and purpose (Zeller, 1999). Indeed, throughout the course of data collection, interview questions were shaped by my interactions with participants and, in responding to my questions, participants spoke about thinking of things in a new way or noted that a new dimension was added in their consideration of what was important. While as a participant in this hermeneutic process my perspective contributed to meaning here, this meaning was confirmed or altered by other participants as they reacted to field notes and the preliminary case report. As trustworthiness and authenticity are the dimensions upon which this research will be considered, a method of reporting which can best highlight the interplay between the participants and the researcher/ participant while allowing the reader to probe for internal consistency is called for (Lincoln & Guba, 1985; Rodwell, 1998).

Before getting to the specifics of this particular case study, it seems important to say something about the responsibilities of both the reader and the writer of the case report. In this process, assessments have been made not only by me, as the researcher. My advisor, peer reviewer, auditor, and the research participants have all viewed the work at various stages from their unique perspectives. While it is the usability, rather than generalizability, of the research that is important here, the reader's assessment along those lines is also important (Rodwell, 1998; Seidman, 1998). The case study is written in a style that uses language not as a means for simply conveying information, but as one that attempts to contribute to clarity by means of a dynamic relationship involving reader,

writer, and context (Zeller, 1999). Rather than attempting to fix a particular meaning for all time, here the reader is invited to use meaning grounded in this case study to better understand and consider concepts that, at times, may seem to be at odds with one another (Balfour & Mesaros, 1994; Farmer, 1998; Farmer, 2002). The reader's perspective, then, contributes to meaning, as what is determined to be relevant by one reader for one context may be different from that of another. However, for this to happen, the reader must be willing to fully engage and allow him or her self to be caught up in the story (Rodwell, 1998). My hope is that the story that follows allows for that kind of engagement and rings true as the reader becomes part of the context (Guba & Lincoln, 1981).

The inquiry data have been organized in terms of four major categories: *What are you trying to do?*, including all data relating to mission and desired outcome; *Security and Technology Issues*, consisting of data regarding access, security programs, technology, legislation, implementation problems, and risk assessment; *Language and Framing*, incorporating all data relating to language and the way information is presented; and *Balance and Trade-Offs,* including all data relating to issues of individual freedom in relation to public safety. Each of these categories is then further sub-divided into numerous sub-categories. Acknowledging that meaning and usability of the findings conveyed in this report will be the result of an intersubjective process that includes the reader's perspective, I offer here a framework for considering the multiple perspectives encountered within the context of information security policy development in the form of a conceptual map.

The need for a map such as this became evident to me when, in the process of data analysis, I realized that data reduction could only take me so far. Rather than finding a way to explain a process of data reduction, what I needed was a way to capture the complexity of relationships, not only within the overall context of the research, but also within the internal contexts of each of the stakeholders under investigation: the *university, private sector, nonprofit sector,* and *government*. Each of these stakeholders can be seen as having its own unique *power*. The university's power is characterized by an open environment that fosters academic freedom, intellectual discourse, and non-biased research. The private sector's power, in addition to economic power, is observed in its freedom. The nonprofit sector's power comes from its values and the government's power is in its ability to mandate action. However, the ways in which these entities interact appear to be so complex that it would seem to be impossible to consider them in isolation.

As I searched for a way to visually represent the connected nature of interaction I was finding in the data, I came across an approach that allowed me to consider each data unit in terms of where it fell within four interconnected concepts, which can be depicted as quadrants. The concepts represented by the quadrants are *subjective,* including opinions, suggestions, and questions of participants; *intersubjective* ,including responses of a cultural, moral, or ethical nature; *behavioral,* including concrete action or response taken to resolve or prevent problems; and *structural,* which included formal responses such as policies, procedures, and laws (Wilber, 2000). The data, while divided into categories and sub-categories according to themes, could then also be considered in terms of these meta-categories. Figure 2 shows the presence of these quadrants in each of the stakeholders. As

the university, private sector, nonprofit sector, and government all interact in ways that fall into the subjective, intersubjective, behavioral, and structural meta-categories, lines connecting them encompass all of these facets. It is my hope that this conceptual map will be useful in reading the case study.

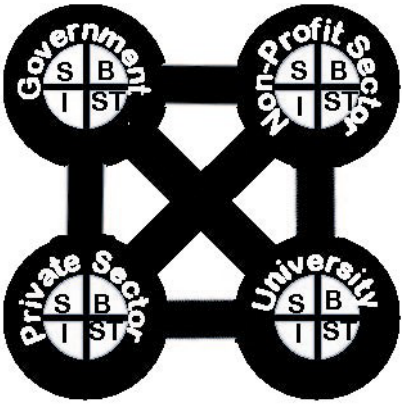

Figure 2. Stakeholder Interaction.

In this inquiry, research participants were assured that every effort would be made to preserve confidentiality. However, I discovered that this was difficult to do when some of them had very high profiles and could be easily recognized if I were to even mention their places of employment. In that the positions of the participants seemed to matter to the story complicated things further. I hope that this has been resolved by using composite characters with fictitious titles that seem to maintain integrity in telling the story. Composite characters have been drawn from the four stake holding groups described above. So, when a character is representative of more than one participant, those participants are all from the same group. In every case, there is more than one character

for each group. This is a result of responses that were not similar enough to attribute to one person and still maintain credibility of the case report. Development of characters and story, in terms of appearance, attitude, background, and surroundings came from material in my field notes. Aside from the challenge of maintaining confidentiality, another occurred in finding a setting in which I could realistically place all of these characters and have them discuss issues related to information security policy, while giving the reader the "flavor" of this research experience. I decided to do this in a conference environment that involved a series of panel discussions, both allowing for a believable setting and for the element of time passing that seemed important for the research experience and the hermeneutic process. A list of characters appears below, followed by the case study, where they are all assembled for the first in a series of discussions on issues surrounding information security policy development.

List of Characters

Lois Lassiter is the organizer of the conference series and represents the researcher. Her thoughts and actions represent my experience in this context.

Community College

Jack Bailey is president of a rural one-campus community college in Virginia's Shenandoah Valley. He has a warm, friendly, and open manner.

Leonard Dalton is vice president for information technology at a large community college system headquartered in Richmond, Virginia. He is friendly, but business like and surrounds himself with the latest technological devices.

Trish Franklin is an IT (information technology) manager at a multi-campus community college in northern Virginia. She has a military background, is well organized, and speaks briefly.

Lydia Johnson is acting director of information technology at a multi-campus community college in the Richmond suburbs. She is not a technologist, but is working on the college's contingency plan and describes herself as a "translator."

Large Research University

Karen March is vice president for security and technology policy at a large Virginia university. She has been working with technology related policy for years and is involved in several university consortiums in the areas of technology and security.

Alice Thompson is vice president for information technology at another large university in Virginia. Her degrees are in English and she claims to have been hired in information technology as a translator and speaks from a "big picture" perspective.

College and University Security Institutes

Mitchell Posner is associate director of security studies and technology at an ivy league school. He is involved with research as well as running a center with a national focus on public policy and cyber-security issues. His background also includes top secret work in government and industry.

Sophia Martinez is director of information security policy at a university security institute in Virginia. She is a political scientist and speaks very candidly. She works with technologists and describes hers as the voice of public policy.

Federal Government

Rick Smith is counsel to a House sub-committee dealing with Homeland Security issues. He is a Democrat with a friendly but business-like manner. His office is in the Rayburn building in Washington, DC.

Carroll Trask is director of strategic planning for critical infrastructure protection at the Department of Homeland Security. He is very outspoken a very enthusiastic participant. His background is in law and private industry and works in the Commerce building in Washington, DC.

Related Non-profit Organizations

Arnold Madden is director of the office of ethics in information security planning. He has a background in law and has also spent a number of years working in a large university. He currently works in an organization concerned with ethical issues of technology and security and is also working on a doctorate in Education. His office is in Washington, DC.

Brad Martin is director of a non-profit organization with the mission of preserving constitutional rights and civil liberties. He works out of a small office in Richmond. He is very friendly and has a good sense of humor.

John Ripley is a senior fellow and director of technology policy at a non-profit, bi-partisan, international think tank. Considered an expert in global technology policy issues, Dr. Ripley was previously in the Foreign Service and has worked with the National Security Council. He currently works in Washington, DC, is very knowledgeable and approachable.

State Government

Mike Dobrosky is state secretary for technology strategy and planning. His agency is responsible for developing standards and auditing state agencies. In addition, he is involved with the recent merger of a number of state agencies into one technology utility and is interested in finding a "common language" to work with this group.
Roger Trent is state secretary for educational technology. He is in the governor's cabinet and works with educational technology policy. His office is located in downtown Richmond.

Private Sector

Matthew Barnes is president and CEO of a small firm specializing in technological master planning for communities and regions located in southwest Virginia. Formerly with a large Virginia university, he frequently speaks to community groups.

Bob Moseley is a security expert for a private company working on Department of Defense contracts. He is retired from the military and formerly worked in the Pentagon.

What is the Meaning of Security? : A Case Study

Lois Lassiter couldn't believe her good fortune. Organizing this series of panel discussions on information security policy issues had been a real coup. For the past year Lois had been traveling throughout Virginia, into Washington, DC, and even as far away as New England, to interview policy makers and technologists from colleges and universities, federal and state government, private industry, and the nonprofit sector about their perspectives on what is important in information security policy development. When

she'd received a grant to fund a series of lectures in colleges throughout Virginia, Lois became very excited. She knew she was up to the challenge of rounding up a diverse and interesting group of participants and looked forward to getting them all together in one place. Until she'd begun her research, Lois had had no inkling of the depth of the issues with which she was dealing or the wide range of perspectives she would encounter on this project. Now, as she sat back waiting for the first panel discussion to begin and thought about all she'd heard over the past year, she realized that her own perspective had been transformed over the course of this process and looked forward to seeing how others would respond to what they'd hear today.

The first session was entitled, *Information Security: What Are We Securing?* Over and over, it seemed that Lois had heard variations on this theme [1]. Some people had had seemingly simple answers to what they saw as straightforward questions. For others it appeared to be more complex, and for some, issues of information security policy raised additional questions. Depending on whether this was interpreted to be a question of securing data, protecting investments, protecting culture, or providing for trust, policies developed to answer these policy questions would be different, as well as who might be involved in attempting to address them. Was it a legal matter? Should private industry be involved [2]? Before introducing the panelists, Lois spoke of how her research, begun in the university, was really only a piece of a larger picture and that she hoped hearing a variety of perspectives would offer us all a way to experience our own roles in new ways . She made the introductions short, took her seat, and listened intently as the program began.

Program #1: ***Universities, Colleges, and Information Security: What Are the Issues? What Are We Securing?***

Dr. Posner began the discussion by talking about the role of the university in shaping public policy. "Colleges and universities tend to have people who think deeply about issues and, perhaps can leverage some of that deep thinking about real life issues more easily than policy makers, individuals or government. The difficulty is for them all to get together and have practical results. People who have good thoughts can help shape policy. As a general rule, colleges and universities have a more unbiased view. They don't have a dog in the fight, are less likely to be biased or influenced by others than business and industry, and are a good neutral player in the implementation of the use of technology affecting society [3]." "An important role for colleges and universities at a time like this is to be what they have always been, bastions of free speech, willing to offer alternatives," joined in Brad Martin. They are important as places to remind us about liberties. Historically, the university has served as a foundation for the marketplace of ideas. Students and professors are expected to explore new horizons. College campuses are created to be free thinking structures, but they can also be subject to politics, especially state universities that depend on government funding [4].

Secretary Dobrosky highlighted the need for government to partner with colleges and universities. "The state is, in my opinion, woefully wanting in terms of the security of our technology. I think the same is true of the federal government." He went on to speak of recommendations of the Secure Virginia panel, chaired by ex Lieutenant Governor Hager. "This is our version of Homeland Security in the state." *The Critical*

Infrastructure Protection Project and partnerships such as James Madison University's *Commonwealth Information Security Center* were mentioned specifically, in terms of best practices and leading edge thinking. "We are interested in a University of Virginia research project funded by DARPA (Defense Advanced Research Projects Agency) and are looking for a place in the state to pilot it. The project involves software that facilitates early identification of widespread coordinated terrorist attacks [5].

Sophia Martinez spoke about how grant funding had enabled her university to create their security center. "First, there was a state grant from CTRF (Commonwealth Technology Research Fund), which offered money after 9/11 for research in the area of computer security. Because our school offers a masters in computer security, this was seen as an opportunity to compete for a grant to develop research in that area." Those already involved with the formation of the security institute, Dr. Martinez explained, had invited her to participate in the grant writing. "I told them I'd be happy to do that" she said, "but that they would have to understand that, as a policy person, I would be putting a public policy/ public interest spin on the proposal and had an interest in the tension between security and other areas of public interest." The proposal involved the fermenting of hi-tech industries in Virginia, which would then lead to computer security firms in the area and the certification that goes along with that. The university received both the CTRF grant and federal funding [6].

When the subject of economic competitiveness came up, Mitchell Posner chimed in, "The market is a powerful force and affects the political process as well as people in other countries. It's a global infrastructure [7]. He went on to talk about both his school's

security institute and another project they've been involved in. I3P (Institute for information Infrastructure Protection) has a national focus and addresses public policy issues in the area of cyber-security. "This came out of the federal government in the late nineties. The question was asked, 'Who is looking out for the protection of our information infrastructure?' and the answer was, 'No one.' A significant need was identified that the market might not take care of fast enough and a thought consortium or 'go to' place outside of government was created [8]."

Up until then, Karen March had worn a thoughtful expression and seemed to be perusing some of the lovely art work that hung on the conference room walls and throughout this new building at George Mason University. She now spoke up about federal research grants. "The funding issue is very important. At a national level, we are presenting the case that education is doing what it needs to do to make our institutions secure. We're working with Microsoft to educate them about higher education needs so that products can be adapted to the university and contribute to a safer environment [9]."

"Colleges and universities work with us to help us move forward." Roger Trent, Secretary of Educational Technology, spoke about cooperation between universities and teacher education in the state, mentioning the University of Virginia, Virginia Commonwealth University, and Longwood University specifically. Training administrators in security issues was listed along with teacher licensure and more traditional kinds of partnering. "Recommendations were made by the president of Longwood, who led the panel, on how data would be collected and then interfaced with university data," he added, "These are sensitive data that need to be kept private [10]." Dr.

March and Dr. Bailey both spoke about the need to partner with other agencies in the community. "You need to draw a broad link between information security and a broad concept of security and safety. I doubt that there is anyone now, after what we went through last summer with Blaster Worms, who has not been made more aware. This has helped us to draw that link. We've partnered with our police department," said March [11]. When a need was identified to develop policies and procedures to work with these other agencies, CIRT (Computer Incident Response Team) was created and works in conjunction with outreach, awareness, risk assessment of technical resources and working with schools, rotary clubs, and other community organizations [12]. With the mention of CIRT, there was some discussion of higher education institutions collaborating through VASCAN (Virginia Alliance for Secure Computing and Networking) and I3P to develop security measures and standards [13]. "To a certain extent, we're constrained by law," Dr. March added. She mentioned FERPA (Family Education Rights and Privacy Act), also known as the Buckley Amendment, which does not allow schools to release student information to anyone but the student. While, on a national level, she continued, there was concern that there will be legislation enacted requiring research institutions to implement government agency standards in order to receive federal grants. "It could cost each research institution millions of dollars to come up to the government security standards and we don't believe that federal standards are the ones that would make our networks most secure," she added [14].

Lois considered these responses in the context of the question and thought about the role of the university which, of course, was where her own interest had begun. While

colleges and universities partner with government in research projects, they contribute to efforts to secure public safety, the critical infrastructure, and national defense. At the same time, they work to preserve their role as a neutral player in developing public policy and places to remind us of our liberties, while engaging in other kinds of partnerships with each other and with law enforcement. As they do all of this, they work to protect data, information, networks, computers, and student privacy, while complying with government information security standards. It was not a simple question, Lois knew.

It was time for a break and, as Lois sipped her coffee, she made her way through the lobby, glancing at nametags and tuning into conversations. "If someone were to gain access, information about grades, student status, and student accounts could all be changed," she heard one community college dean say [15]. "But, it's not only about disclosing information and gaining electronic access," her companion added, "If you have information on a laptop or confidential papers are left lying about, you have the same result. This gets us into the area of physical security [16]." A common thread throughout the entire group seemed to be the importance of including physical security in information security planning and policy development [17]. Roger Trent, Secretary of Educational Technology, turned to listen to the gentleman on his right, from the Department of Homeland Security. "The big business challenge and the policy challenge," he was saying, "is to encourage and inculcate an environment of security consciousness to protect a way of doing business [18]." Dr. Posner, one of this morning's panelists, replied that in his e-commerce course, they consider case studies that give assurance of privacy [19]. Trent joined in, "Governor Warner wanted more data about what is going on in schools. This set

the issue for us. Right now we have an RFP out asking vendors to show how they deal with security and student information [20]."

As she continued making the rounds, Lassiter heard about protecting personnel records and donor lists, as well as students on the Internet. Dr. Bailey, the community college president from this morning, joined others in talking about the physical safety of faculty and staff, more shredders on campus and how they'd all become used to increasing levels of computer security. The tall gentleman to his left with the brown leather jacket and the Washington, DC nametag, was talking with Sophia Martinez and stressed the importance of document protection and Dr. Martinez concurred with so many others that problems of records and record-keeping, along with what to do about data were among the biggest security issues for universities right now [21]. The crowd started heading for the next session and Lois began to hear some talk about protection of critical infrastructure. "The private sector needs to take a leadership role. People in industry are the stakeholders. Anywhere from eighty to ninety-five percent of the critical infrastructure is owned by the private sector [22]." One of the participants from the Department of Homeland Security joined in. "In critical infrastructure protection, you have to have three basic objectives: economic security, public safety, and national security [23]." The two gentlemen at her side joined in this discussion. "Tom Davis, the Virginia representative from the House of Representatives is leading the forefront for cyber-security efforts for the government," one of them said [24]. "Networks are one part of the critical infrastructure," the other added. "The cyber side is what is being emphasized [25]." Both set their coffee cups down and headed for the auditorium.

Lois Lassiter began by welcoming everyone back and explained that, for the afternoon's program, panelists would be divided into groups representing college and university, government, the private, and public sectors and that we would hear from a representative from each group before they engaged in a general discussion. "Without further ado, I will now turn the microphone over to our panel, beginning with Dr. Alice Thompson, from the university group. I hope you all enjoy the discussion. Thanks again for coming. Dr. Thompson…" "Thank you, Lois. Well, in my mind, it goes to information technology as part of the trust equation. You could latch down your systems as if no one had trust in anything that the system does or in a person's ability to make judgments about what the system delivers. But you still need to be able to understand what systems will and will not do to use them responsibly. You still have to be able to discern good information from bad information. A system cannot do that. That is a very human function. A technology system will only do what humans program it to do [26]."

"Yes, my name is Mike Dobrosky and I am here representing the state government group. It's interesting that you should mention that, Alice. Very often breakdowns in security don't have anything to do with technology. Hackers get more publicity, but people don't realize the high incidence of internal threats. Maybe an employee decides to engage in something he shouldn't or be lazy about changing a password. They might even put a sticky note with the password right on the computer. This is really where the problem is most persistent [27]." "Good afternoon. I'm Leonard Dalton with the community college group. I'd agree that technology is the easier part. The hardest part is making people aware. If I leave my credit card statement lying around, I could have

MacAfee on my computer and my house in lockdown, but if I throw my credit card statement in the trash and it gets taken outside, that information is not secure [28]."

"Bob Moseley here; private industry. What I see as important here is the relationship of humans to machines. The relationship between technology and security, from my standpoint, is that you want to apply technology to make security better and reduce the use of humans to do security. For instance, if you want to control access to an area, you could put a guard on duty to check ID cards. There have been some studies that show that guards are not very good at this because they don't know what they're looking for. Another option would be to have a biometric entry point where someone would be identified by a thumb print or an iris scan. Here you have made security better and you have eliminated the human factor. If you have as security gate, you can use a combination of something that identifies a particular car and a fingerprint that will identify a specific driver. Here you have a positive ID and you have eliminated the need for a guard at the gate [29]."

Dr. Martinez spoke next. "Well, from the computer nerd perspective, computer security can be seen as a sequence of prime numbers, algorithms, etc. When you step out of that into management, there may be a recognition that there is a trade-off between the complexity of the system and the people who use it. A less complex system may actually be more secure if people are more willing to use it [30]." Arnold Madden, from the Office of Ethics in Information Security Planning, was nodding his head and writing something down, but it was Carroll Trask from Homeland Security who spoke next. "I don't like the word 'security', but I'll use it here to illustrate. Technology is part of security and security

is built on a shaky foundation. It has three legs: people, policy, and technology [31]. Technology is not necessarily the cause of major breaches. It's the people and the business processes, but that is hard [32]."

John Ripley, our think tank representative, was the last on the panel to speak. "Relating security to technology, I see this as three levels. At the first level technological advances and use of technology provides and has provided a military edge. U.S. security has rested on military technological advancement. This is a broad linkage. The second level has to do with technological change and national strength. Here we're looking at the broader strategic aspects of national competitiveness. If new technology increases productivity, this will make for a wealthier economy which can then afford a higher degree of security. The third level involves the use of existing technology to improve security, in part, Homeland Security. Can we find ways to use network technology to improve Homeland Security [33]?"

Well, again we had quite a range of perspectives on the interplay of security and technology and it was apparent that a good discussion would take place. Over the next forty-five minutes, participants asked questions and responded to what the panelists had said. There seemed to be a consensus that the people piece of this was very important. Colleges and universities all seemed to have educating users as a part of their security programs. "If people try to circumvent technology, it won't work. The human factor is difficult to control. Firewalls are a big security sham. They won't help if an employee does something within an environment," commented Dr. March [34]. The give and take continued for awhile until someone referred to the panelists as experts and Sophia

Martinez and Alice Thompson spoke at once. "There's an idea that experts know better than the average citizen. Experts are extemporizing. It may look good, but we don't really know [35]." "Most people do not have a clue! Just because people talk about high and low bandwidth doesn't mean they know what it is or what having high bandwidth might allow you to do differently [36]."

Karen March spoke about how her degrees in computer science and hadn't necessarily prepared her for coordinating the large decentralized information technology department at her university and how she'd been given the responsibility for IT policy just a year ago. "It's been a rocky year learning how difficult policy is. I'm not an expert [37]." Both Lydia Johnson from the community college group and Bob Mosely, from the private sector, had similar comments. "Public policy in education includes those who feel they are an authority on school because they went to school," said Johnson, "Policy makers don't have expertise and, depending on who they listen to, may not get good information. Policy makers often make policy about things they don't understand [38]." "Everyone wants to be a security expert because it is very popular," added Moseley, "They think that, because they were Marines, for example, that they're an expert, but they're not. I can pretty quickly figure out who knows what they're talking about with regard to security, but I could be revealed as a fraud by an IT guy. I know this only from the point of view of the user [39]."

Mike Dobrosky, Secretary for Technology and Security Planning nodded his head.

"I have some experience with Homeland Security technology, and higher education in the state and, in my opinion, the state is woefully wanting in terms of the security of

technology. I think this is typical of all states from talking with my peers. The same is true of the federal government. There seems to be a quiet desperation of Homeland Security folks at all levels to fix the problems and outsmart potential terrorists [40]." Lois wondered what our Homeland Security participant would have to say and he spoke up next. "In 1998 ISAC (Information Sharing and Analysis Center) had a very specific meaning. It had to do with collecting, disseminating, and analyzing data. Now an ISAC is everything and the kitchen sink, including risk assessments. These are meanings that were never intended. That's the culture in Washington. ISAC is in vogue. The original intent got buried. I get very irritated. Information sharing is really about taking action. The endgame became information sharing, a process rather than a deliverable. It's really warped [41]."

Discussion continued about how one might determine who is an expert, ASIS (American Society of Industrial Security) certification, and other criteria. It is very difficult, with information security, they agreed, to even know what the risks are [42]. Our time was up, but Secretary Dobrosky brought the discussion on experts to a close by saying, "I wonder sometimes if security isn't an illusion and the fact that we feel secure is only because we're ignorant of what threats may lie ahead. Maybe ignorance is bliss [43]."

As Lois shook hands with people and they all prepared to leave, she overheard much about the issue of educating users and how most of them do not realize what the dangers are. In a general discussion of threats, Karen March added, "When a crisis occurs, like 9/11, I would rather know what the dangers are. I'm kind of in agreement with the

NRA on this. I don't agree with the rest of their stuff, but they provide a safety course that gets the point across [44]." Others seemed to feel that educating users is not as easy as it sounds and that real learning and change can be quite difficult. Two of these were Lydia Johnson, Acting Director of Technology at a community college and Alice Thompson, Vice President of Information Technology at a large university. "What are we doing to prepare people for change [45]?" Dr. Thompson stressed the importance of lowering anxiety that works as a barrier to innovation and making ourselves more accessible to change. "Today's technology systems offer opportunities for new approaches to life and work, but people have to understand what technology might allow, decide what they want to accomplish with it and figure out why it is important to accomplish certain things in new ways [46]."

So it's not only to do with what we are protecting today and how we are using technology right now, Lois observed, it seems that we have to leave room to consider what we don't yet know. How do we keep from limiting ourselves as we make decisions from day to day? All that talk about not knowing who the experts are reminded Lois of discussions about the growth of knowledge. Is it that the experts are limited by parameters of old disciplines that may not always be applicable? How did one reconcile issues and problems that seemed to require concrete solutions in the here and now with ethical or cultural concerns about uses of technology for security? The next program would begin by dealing with issues of access and Lois would keep these questions in mind as discussions took place and information security policy decisions were discussed.

Program #2: *Using Technology for Security: Issues of Access*

This program, hosted by James Madison University's Commonwealth Information Security Center, would meet in the ISAT (Integrated Science and Technology) building. As Lois drove over the Blue Ridge Mountains on her way there, she thought about issues of access and hoped this was a good starting point for a discussion of issues and problems of using technology for security. She'd noted in her interviews that access had been important for those who spoke in technical terms about passwords, as well as for those who were concerned with broader issues, such as a citizen's right to know and those with legal concerns who spoke about *Freedom of Information* laws or those concerned with limiting access and discussed *FERPA (Family Education Rights and Privacy Act)* and *HIPAA (Health Insurance Portability and Accountability Act).* Lois planned to keep all of this in mind as she listened to today's panelists.

After their earlier discussion on access, Lois had asked Alice Thompson to lead today's session and she had agreed. Alice started off by talking about an old friend of hers, Bob Hetterick, with whom she'd been discussing information technology for years. "He could be very funny," she began. "He used to use a graph with an *x* and *y* axis and a line going straight up and no descriptors for *x* and *y*. [The audience laughed.] A theme running through his work was the trade-off between access and privacy. For the last fifteen or twenty years, he's been saying that, any way you looked at it, this is one of the trade-offs when integrating technology with the content information people use in their lives and work. I'd have to agree with Bob Hetterick about this constant balance between access and

no access[47]." Dr. Thompson looked to her left, turning the floor over to Carroll Trask from the Department of Homeland Security.

"When you talk about 'academic freedom' and 'openness,' consider this," he said, "If you're a hacker and you want to get lost in the maze, you look for the suffix, *edu*. You go through the colleges and universities. The reason for this is that their computer systems are very open. The policy reason is touted as academic freedom and assumes that those using it have good intentions. This is very different from the security system at a store in the mall. The storeowners also want you to come in, but they want you to buy. They want to increase revenue, not lose money. They have cameras that watch you and some major credit card companies require store owners to take strict precautions with their point of sale customers and check on them. In the financial services industry, their interest is in data protection. The weak link is the college or university. This creates a debate in academia about access v. security. I recognize that there is a tension. A balance needs to take place [48]."

Dr. March spoke up. "My big fear is that I won't know when information is compromised in the commercial sector. Higher education is depicted as being a vulnerable and unsafe environment in IT (information technology) terms, because we're oriented toward open access. The truth is, we are more secure than most of the commercial world. This has to do with our revealing our failures and the fact that we don't go out of business if something goes down. I may lose my job, but the college is not going to close down. In the commercial world, with a failure at MasterCard, for instance, where is the incentive for commercial vendors to report that? They may go out of business. It's really the exact

opposite from current thought. We had a security incident at my old job and called in a vendor. They were very helpful and were able to tell us how they thought intruders got in. When we asked the vendor about what their commercial clients had reported, they told us that their commercial clients would never reveal this, would never report it to them. Medical centers and educational centers are more open about security breaches in their systems. Have you heard of PKI (Public Key Infrastructure)? It's associated with smart cards, advanced security devices, and electronic signatures. I went through this debate, about the commercial world and how they are not as secure as the academic world, with state government officials who believed vendor allegations that higher education is not secure enough to run these systems [49]."

The discussion was now well under way and Lois had heard comments that ran the gamut from methods for allowing access to the difference between access and authorization the way many schools have split their networks [50]. Carroll Trask, from the Department of Homeland Security, had something else to say about the access v. security issue. "I think there are probably two standards, if you will, in colleges and universities in terms of the academic organization v. administrative organization. The administrative organization probably needs to be a little less open because of the categories of information they deal with, such as revenue sources or personnel information. On the academic side you have research projects and more of a sharing environment. There is less critical information in terms of financial information and things like that. I don't doubt that there are research projects that need to be kept private, but that is the exception rather than the rule. The main issue, to sum it up, is that the two different organizations and their cultures

probably require two different approaches to technology security. There is a constant tectonic shift [51]."

Others concurred. "In an open environment where access is important, any security policy should be based on what people need to know to get their jobs done. How do I make sure Lois has access to what she needs and not to other things?" said Leonard Dalton [52]. "University issues have to do with disclosure of information or privacy rights of others. We have twin devils," added Karen March, "On the one hand, you want to be as open as possible, but you can't disseminate all information. It's a little schizophrenic [53]." Secretary Dobrosky, agreeing that security was a challenge, pointed out that the concept of balancing access and privacy is one of the guiding principles of enterprise architecture, from which statewide standards are determined. Bob Moseley, who works in a private sector environment developing security solutions and had also been assigned to the Pentagon while in the military, added, "It's hard for me to get my head around this stuff. In business and in the military you have two different ways of looking at the world, making money v. doing the right thing [54]."

"Many universities are taking the approach of having secure enclaves; records, for example. This is seen as an exception to the traditional open environment of the university. Another exception might be in biological research, for instance. Possible patented information may be taken offline," Trask added [55]. Along with more comments about the importance of access in higher education, were concerns about DOS (Denial of Service Attacks), viruses, worms, and identity theft. "The things we have to think about when developing security strategies are the cost/ value equation, the culture, and the clash

between the open access to information tradition of the university and the controls needed for effective security [56]," added Dr. March, Vice President for Security and Technology Policy from one of the large universities. Lydia Johnson, Acting Director of Technology at a suburban community college, added that another missing piece was making sure that we had good information in the first place and said that we really don't talk much about the credibility of the data we're protecting. "What criteria do we use? We could be protecting and disseminating bad information. How do you ward off vulnerabilities and threats when new data are collected [57]."

Carroll Trask again had the floor. "Colleges and universities need to strike a reasonable balance. One thing that will help reach a rational conclusion is *downstream liability*. This has to do with an attractive nuisance, resulting in danger, peril, or damage to an unintended victim. An example of this is an open swimming pool on private property. There may be a sign saying keep out, but on a hot day, the neighborhood kids won't read the sign and the owner is held liable if someone is injured or drowns. But, what if the water is not treated, the kids go in the pool, get SARS (Severe Auto Respiratory Syndrome), and they go to school and give it to seventeen other people. The pool owner will be held liable. This is an example of *downstream liability* [58]."

"Colleges and universities get money from students, government grants, and federal funds," Trask added. "These are all linked through e-commerce and you could, theoretically, back in and get to a bank. This has been done. Here is an example in the college or university. Suppose a hacker takes advantage of the open environment to get into your records. He knows someone at the school whose wealthy uncle pays their tuition

and he wants to find a way to get access to their money. The hacker may be in Libya or India and is unreachable. However, faulty security of the school, which has allowed this to happen, makes them liable. So far there is no case to prove this or test it [59]." Dr. March then made reference to a case involving two GMU students who had hacked into the network in the late nineties. Not only was the case thrown out of court because the school didn't have policies in place, but the students counter-sued and the university ended up settling out of court [60].

It was almost time to end for the day and Lois was just about to say so, when Carroll Trask spoke up about liability concerns for colleges and universities. "Suppose I work for a company involved in research involving the Human Genome," he said. "Because of my trusted relationship with your university, I will provide researchers with data to use in their research. Now, because of faulty security, this is stolen by my competitors. As for the university, you can't say that ignorance is bliss. The time for ignorance is over. A jury is not going to believe a CEO (Chief Executive Officer) who says that he never expected the system to be hacked into [61]." As the group headed out to the break room, Lois seemed to sense some disquietude among the group. She suspected that it might be the frankness with which the liability issues had been expressed. She hoped that an open dialog would continue and that participants wouldn't branch off and limit their communication to only like-minded individuals. Once again, Lois was intrigued by the path this discussion had taken. The panel had begun with the concepts of access and security, or limiting access. Then, in considering technological applications of security, Lois noticed that surveillance, for instance, raised questions about individual

privacy. Also, while reference to patented information and connections of e-commerce to the university environment seemed to favor greater restriction to access, discussion over Public Key Infrastructure had introduced the notions of disclosure and non-disclosure and questioned whether an atmosphere of non-disclosure really contributed to a more secure environment. In the second part of today's program, we would hear about security programs and policies, which were already being discussed by participants, as they enjoyed refreshments.

As Lois helped herself to coffee, Jack Bailey, the community college president joined her. He was saying that, while he thought it was important to include all those affected by a policy in developing it, he also thought that in the area of information security, policy development needed to start with those with technological expertise. "I'm concerned that this might sound like a top-down method for developing policy," he said, "and I really believe that policy should be developed from the bottom up. But in the area of information security, when computer technology is such a large part of that and there is so much information in the computer, there are just certain people that you have to trust with knowing about vulnerabilities [62]." Before Lois could respond, Karen March joined them, adding that you could not consider security in isolation, but needed to consider the business, the users, and the technical environment. "You need to have both integrity of data and integrity of processes," she added [63]. "And there also has to be a commitment to security," added Leonard Dalton. Some of the other participants joined in. "Policies and procedures have to do with how security is managed and technology has to do with mechanisms for how they enforce it," Lois heard someone say. "This includes physical

security, such as who can literally get the key and go in the room, as well as hardware, software and its manipulation, and elements of training, testing, and auditing [64]."

It was time to go back in for the second part of the program, but there was a slight delay, due to technical difficulties. "It figures," laughed Lois to herself. Those around her must have been thinking the same thing, because now talk turned to technology. Technology did not just have to do with computers, Lois heard several people say. Just as it seemed the technical difficulties had been taken care of, Secretary Dobrosky seemed to sum up. "In its broader sense, I see technology as being anything that can be done in an automated fashion with some level of intelligence. The fact that my clothes are dry and I don't have to re-set the timer. That kind of thing is becoming more and more ubiquitous [65]." People began setting down their cups and heading back into the room where the discussion would take place. Lois found herself between Leonard Dalton from the community college system and Alice Thompson from the large university who had spoken earlier and she heard too very different definitions of technology. While Leonard pointed out that in the information technology world, the word *technology* refers to new innovations, Alice took more of a big picture approach. "I don't think of technology as a mechanical thing," she said. "It can be, but technology can be an idea too," she added, "There's an economist, Paul Romer. He's one of the few economists that looks at the idea of technology. If you are thinking about technology as an idea and the things (knowledge and knowledge-based organizations or services) that spring from an idea, you have a different approach to economics [66]." As the crowd was being seated, several people agreed that it's not the technology itself that matters so much, but what you do with it.

"These are the *what* and *why* questions," Alice Thompson added. " To what end, technology [67]?"

This made for a nice transition into the technical aspects of security programs, Lois thought. Once she got the program back on schedule, several panelists discussed a variety of technological security devices, including controls, filters, master accounts, and passwords. Acknowledging that things had become more difficult since a greater number of computers have become networked, they spoke of additional layers of security and how technology allows us to automate, but cannot improve on a poor manual plan [68]. Mention was also made of the new vulnerabilities created by technology and the new security risks that have been created, as well as how our expectations have changed with regard to communication [69]. Along with encryption, data transmission and telephony were described as huge security issues. "How do you use technology to its advantage and still have at least similar security to mail and phone?" asked Rick Smith, the House Counsel [70].

As we got into examples of technical applications for enforcing security through the use of DNA, eyes, and feet, Secretary Dobrosky took that one step further. "The other day I was talking to a colleague," he said, "and mentioned that I could see a day when my grandchildren would have a chip embedded. I don't know what exactly it would be used for, but I wouldn't be surprised to see that happen. My friend was shocked by this [71]." While references were made to "dumb" or "bad" applications of technology, Karen March pointed out that, whether or not the intent is malicious, the same procedures that work for malfunctioning can work to respond to threats [72]. Lois saw this as a possible distinction

between information security and information technology issues and Matthew Barnes, who ran a small firm specializing in master planning for communities and regions, spoke about how issues of access and authorization might or might not be technical issues [73].

It seemed that folks could go on and on about the uses of technology and Lois was just as happy to have Leonard Dalton change the subject and begin talking about laws that were written around technology. He was referring to the fact that we can't reproduce and distribute digital copies without penalty the way we could with paper copies, but that was not the only example. "The law is written too narrowly," added Karen March. "A number of states are writing state laws, supported by the motion picture industry, that say that it is a crime to willfully mask the address of a machine downloading movie files. The problem is, this is how a firewall works. It masks the IP (Internet Protocol) address, so it would be a crime to have a firewall installed [74]."

"Legislators have to be careful how they make determinations," commented Secretary Trent. "They have to get advice so they can make good policy decisions, not just for the profitability of an industry. There are a bunch of idiotic laws, the most obvious case having to do with the music industry. The benefactor of the law is a small group, but the implications are for the rest of society [75]." He went on to give another example of proposed legislation that would benefit the television and motion picture industry. "A TiVo," Trent added, "has the capability for you to record every version of the Sopranos that was ever on TV. DVD recorders can create a permanent digital version. This creates a problem for the people who make the TV programs. They are saying that they want the

government to regulate technology so that each TiVo manufactured only has the capability of making one copy [76]."

March described what might happen if the DMCA (Digital Millennium Copyright Act) were taken to an extreme. "I went to a conference in DC last summer and there was a professor there from George Washington University talking about some of the premises behind the DMCA. It is against DMCA for me to try and crack encryption or publicize how I cracked it. Have you heard of Felton? He's a professor at Princeton University who assigned his students to crack the code. They did this fairly quickly and Felton was going to present a paper about it at a conference. He received a 'cease and desist' order and pulled the paper, but then counter-sued, saying they were violating his free speech. The suit was not successful because Felton had only received a cease and desist order and had not actually been sued. Well, according to the GW professor, here is what happens if you extend this idea. Suppose the air force finds an encryption algorithm and discovers that it hasn't been broken. Felton can't tell the air force that the algorithm is flawed. Then the navy or some other party could come along, assume it the encryption algorithm is secure, and also start using it [77]."

Another example of laws written around technology were the UCITA (Uniform Computer Information Transactions Act). Leonard Dalton went on to talk about these "shrink wrap" laws that have been passed in Virginia and Maryland and allow the user of the computer to accept conditions by clicking. "Who reads all of the conditions?" he said. "Most people wouldn't understand them anyway. When you load software on your computer, you click to turn access of your computer over to the software company. How

do you know what they are doing? How far do you trust them? It's like giving a key to a handyman and telling him to just let himself into your house whenever anything needs to be fixed. These are security issues [78]."

Matthew Barnes added, "Another big issue is that more people have access [79]" "I agree," said Carroll Trask. "They expect the users to download patches to improve security and fix problems. This is nonsense. My seventy year old sister is not going to download her patches, but she loves being on the Internet. In the past, there was a very sophisticated user group. Now the user group is not sophisticated, but has very sophisticated equipment. How do you solve the patch problem, the ISP, or the backbone, trying to have automatic downloads? These are challenges. It's extremely expensive to re-do all the software and hardware. There's a wide range of capabilities and interests of citizens [80]."

Copyright was considered from another angle when Dr. Johnson spoke about faculty. "Faculty may create works for research that need to be protected. There are copyright issues. Who owns what faculty members produce? Who owns the knowledge? Technology has changed this. When this material wasn't on-line, it was easier to protect. You could put it in a drawer. Technology has now really made this an issue. It has really exploded [81]." "Institutions in VASCAN (Virginia Alliance for Secure Computing and Networking) are collecting data on strategies that work with resident students," said March [82]." She also mentioned the downloading of music and someone else chimed in, "pornography [83]." While some clearly thought that getting students to comply with the DMCA was impossible, others continued to look for ways to comply and spoke of the

problem in relation to bandwidth [84]. "The big problem for colleges and universities, though, has to do with bandwidth," said Carroll Trask. "This is a limited resource. It's like a pipe or a hose with water coming through it. If one or two people are drinking the water, there is still plenty, but what about hundreds? It's the same thing with bandwidth. If one or two people are downloading, it's hardly noticeable. When hundreds are doing it, it interferes with academic research and academic freedom [85]."

"When we're contacted about DMCA (Digital Millennium Copyright Act) violations," said Arnold Madden, "we agree to follow up with that person. This is what colleges and universities do." "Some students wrote to me about 'Big Brother,'" Karen March added, "if we have a security problem, we have to be able to locate the machine really fast. It also helps us to identify, in addition to those wreaking havoc, anyone violating copyright. It's really a no-brainer. We have to do it. We were prepared for the Big Brother reaction. We don't monitor for content, though. Some universities do. This takes you down a path of no return. With the USA Patriot Act and surveillance, they can request information from an ISP (Internet Service Provider) with minimal justification. You could always get this information, but in the old days, you needed due cause [86]."

As discussion continued, Lois heard panelists speak about decisions related to access and dissemination, who decides what is considered public information, and the issue of office workers who may not understand what is expected of them with regard to confidential material [87]. "Technology does not always do what it promises, especially if your technical staff is not adequate to manage the system," added Trish Franklin [88]. Issues with several applications of technology used in everyday life were discussed and

Roger Trent commented, “Voting last night, going somewhere where they had a punch system, I wondered how secure that card is. I looked it over carefully before taking it to a machine. I have a heightened awareness of the weaknesses of technology [89].” “Technology is similar to guns,” Dr. March added. “It can be extremely beneficial, but can also be one of the deadliest things that ever whacked you. Consider changing identity, for example. What if the state sex offender database is not fully protected? As a joke, someone enters your name and it turns up in a criminal background check. That is a criminal application of technology. The guardian of the information didn’t know how to protect it [90].” She went on to say that even patient care in hospitals could be impacted by attacks on networks and, while Bob Mosley spoke about the nuisance of having to use encryption to pass files back and forth, many heads nodded when Carroll Trask added, “With information security, you really can’t protect and prevent. The range of action is much broader and it’s more a matter of risk management. Physical security is about managing consequences…gates, guns, and guards. Information security is not as clear. There is a much wider range of impacts and consequences that are indirect. It’s not always obvious what the consequences are! You can’t predict everything. Threats and tools are constantly changing [91].” This notion of building in security was echoed by other participants, as well [92]. “You need to build in the ability to respond,” Trask continued [93].

Dr. Thompson spoke about the kinds of automated decision making gone awry that we’ve come across in science fiction and Mike Dobrosky referred back to what he’d said earlier about the likelihood of his grandchildren having chips embedded someday. “On the

one hand, that might be very useful, especially for small children or for teenagers when they started to drive. But once you reached the age of consent, this might chafe somewhat. We're running into many facets or aspects of this conflict between security and privacy [94]." It was time for this presentation to end and Lydia Johnson gave us something to think about over the break when she said, "One of the favorite discussions in the classroom, in medical science, for instance, is that technology has made it possible for us to have the knowledge and ability to do things for which we do not have ethical answers. We haven't caught up with technology. It's a tremendous challenge. It's not only whether you can do something, but whether you should. Some of this is personal and some is addressed by public policy [95]."

Lois was aware that, once again, discussion had not remained in a technical realm, nor was it totally involved with policy and law. While not completely predictable, by any means, Lois was starting to see that each discussion took the participants through the subjective experiences and perspectives of the panelists, technical applications to respond to needs, policy decisions or laws relating to technology, security, or both, and back to ethical, moral, and cultural concerns. Just now, she'd heard about a style of policy development starting with the technical experts, as well as definitions of technology that ranged from the specific new innovations to an idea that offers a new approach to economics. As technological applications of security seemed to become more advanced, consideration of them had also caused participants to be concerned about surveillance and intrusions into privacy and to comment on how technology can be used in a bad way. As she considered all of this, Lois also found it interesting that, what seemed to have been a

narrow focus on technology, had resulted in problematic laws and that there were concerns about proceeding with technological security applications before we understand the ethical implications. After another short break, discussion would continue on risk assessment. Lois fully expected that response to risk, too, would vary depending on what the risks were seen to be and on whether security was perceived as securing networks, investments, culture, public safety, individual liberties, or something else. She looked forward to hearing what the panelists had to say.

After the break, Leonard Dalton began this part of the discussion by talking about the move of organizations toward risk assessment and contingency planning. He spoke of both local disasters that had benefited from risk assessment and disaster planning, as well as making reference to the businesses that had been located in the World Trade Center on September 11, 2001. "After 9/11, colleges were dusting off their crisis management plans and a new interest was placed on the ability to reconstitute and go on," he said. Dr. March spoke adamantly about the difficulty of securing information saying, "Anyone who guarantees the integrity of the data is lying [96]." Carroll Trask responded to this by suggesting that there might be other ways to talk about assessing risk. "My general philosophy leads me to not like the word 'security,'" commented Carroll Trask. " It has a negative connotation. In a business cost center, security could be said to be a way to bleed from the bottom line. How much is enough to spend on security? When I talk to the business community, I suggest the word 'assurance' instead. This leads us to focus on business continuity and to look at money spent on assurance as an investment that enables business to retain their customer base and maintain customer confidence and, ultimately,

add to the profit line, rather than detract from it. Those in private industry are in a position to know how much to spend [97]."

Dr. March replied by pointing out that, "Cost/value is different in the non-profit world where you make do with minimum staff and security is labor intensive. You must ask, 'What am I willing to give up, in order to achieve a certain level of security?' In the business world, you want to protect business assets so that you can continue to make money. Security is the cost of doing business. Higher ed. is a culture that puts its resources into services. It's painful to take money for service to protect against some unknown threat. We don't have a bottom line. When we have security failures, the impact is on faculty, staff, and student productivity. A faculty member may have to stay an extra ten hours to get the job done, but this doesn't actually cost the university money [98]." According to Mitchell Posner, ROI (Return on Investment) was cited as the security argument and information was referred to as the "crown jewels of a business [99]." "People see it as an expense," he added. "I see it as an investment. You're seeking the avoidance of particular types of security breaches and guaranteeing the data entrusted to you. For example, if something has been altered, you want to know who changed it and why [100]." "On the other hand, is what you've got to secure valuable enough to want to secure, as opposed to other alternatives?" added Trask [101].

While most of those in the discussion on ROI thought more needed to be spent to protect information, Matthew Barnes, our community technology planner, pointed out that this is not always the case. "My clients often need a lot of education in order to be able to have a thoughtful conversation about appropriate technology," he said. "Sometimes that's

paper and pencil. I often need to say, 'You don't need to spend more money. You're spending too much.' My work is heavily education oriented [102]."

While Trask made references to profit and a bottom line, college and university participants spoke of how this was different for them. "The states could make every building they own secure," said Karen March, "but what would it cost [103]?" "We are not driven by the profit motive," added Dalton, "but by things like enrollment. We have invested very little in security and it's been the same with most other businesses, except maybe banks. Over the next three or four years, security will become a larger percentage of the budget and there will be more people allocated to securing the organization [104]."

"It's very difficult to justify additional dollars for security to prevent something from happening," claimed Karen March. "It's hard to convince people that things could happen when they haven't already [105]." "In the end, security is only relevant if it protects something you value. If it is cheaper to bring it back up, you'll do that instead of prevent," added Trask. "There is a long learning curve for some people. Your choices depend on what you know and what you can afford. That's when you invest [106]." Secretary Dobrosky added that the state also wants to avoid having agencies spend too much on risk mitigation if their environments don't warrant it [107]. Trask felt that the consumer would demand a safe computer environment. "It's a vicious cycle for the vendor," he said. "In the end, the customer will win, like they did with making the automobile safe. There is a very similar pattern here and the IT industry knows it. But, you know what? The consumer always wins. This is a litigious society and Microsoft has big pockets [108]."

Carroll Trask was referring to a class action lawsuit in California involving identity theft in the operating system. Either this case or another one, he felt, could test whether or not it is reasonable for consumers to protect themselves, as they are currently expected to do by downloading patches, etc., adding that, while the private sector doesn't want to spend the money, consumers will demand it and it will change the landscape and relationships between consumers and vendors. "The private sector goes through cycles," he continued, "This is the mature stage in which the consumer has certain expectations. Lawsuits establish a precedent and it becomes part of the psyche. We expect them to protect us [109]." Even though this would require research and development to find a new way mean to develop software, he seemed quite confident that it would be done.

Dr. March agreed with the concept of building in security and indicated that her staff was currently in the process of evaluating security built in to network appliances, data acquisition devices, and access control cards, "A good security principle is to have security built in from the beginning [110]." Research and development are needed, they agreed. "With the problem of host computer security, 'baking in' security is the answer," Trask added. "If you think about threats, they go through third parties, like your grandmother's computer [111]." While educating users appeared to be an important component of the college and university security programs, Trask favored software research and development, claiming that educating users was not worth the effort, "Raising awareness won't help if those folks aren't sophisticated enough to understand," he said [112].

Discussion went on to include the notion of protecting information as it is disseminated. Trask, Posner, and Madden all made references to HIPAA (Health

Insurance Privacy Act) and/or the FSMA (Financial Services Modernization Act) that call for safeguards of personally identifiable information, as well as encryption, which provides a scrambled path to protect the information that you are transmitting and deterrents, which essentially put roadblocks in the way [113]. Trask noted that information is only valuable if it is used and that there is some risk involved in using it. "The safest car is the one that's parked in your driveway," he added [114]. "I could download the Dow Jones stock figures," said Carroll Trask. "This would be pretty meaningless to me, as I don't know enough about these figures to make sense of the data. However, they would not be meaningless to a stock analyst. Now, do you need to spend money to protect this information from me? No, but data must be protected in transit so that it can't be modified. This is a form of information assurance [115]."

Karen March and Mitchell Posner both spoke about the importance of being able to trust that your banking and credit card transactions are secure, as well as concerns about personal information getting on certain lists and receiving SPAM (Self Promotional Advertising Messages). However, Posner also pointed out that, while we are concerned about on-line transactions, point of sale transactions may not really be any more secure [116].

Rick Smith, Counsel for the House Sub-committee approached information security from another angle by talking about the consequences of not securing information and how these may differ if you are considering policies or laws, including criminal laws, which apply to top secret or government documents. This not only involves protection of information, but how it is handled. "If you put something in a safe, it is secure, but what if

you talk about it?" he added. "Discussions about it might be public or private, in confidence or out of confidence. Does it have to do with a need to know? Is it top secret [117]?"

Mentioning that the *Commonwealth of Virginia Information Technology Resource Management Standard*, Trish Franklin, the community college IT (information technology) manager, spoke about the importance of paying attention to audits saying, "You need to be able to show an audit trail of what steps were taken when an attack has occurred [118]." Karen March added that they had just been audited at her institution and that, with the focus on business continuity, risk assessment, and educating users, that it is very important to get the buy-in of top executives so that all of these objectives can be carried out [119]. Secretary Dobrosky agreed that the auditor's role was important. "They can make the determination as to how well the risk is mitigated in the protection of information." He explained that auditing is really the oversight function for security policy and procedure and that the *Commonwealth of Virginia Information Technology Resource Management Standard* contains specific components to be implemented by every executive branch agency, which includes higher education. "We have the standard and the auditor is the check and balance." "However," he added, the auditors would like the standard to be more stringent [120]."

Several of the university panelists seemed to bristle at this, pointing out that the state standards have been developed on more of a state agency model, like the Department of Social Services, for example, and don't seem to apply as well in a university setting, where there are so many computer systems that the central organization may not even

know about all of them. Other agencies are run more like a business, they felt, while the university operates more on a consensus model [121]. "Well, each agency decides how the standard will be implemented," replied Dobrosky. "The standard is based on standard best practices and the auditors look at your documented security program." While he made a point of saying that the standard was not one size fits all, some of the university panelists felt that is exactly what it was. They were also very concerned that the state seemed to be leaning towards a more prescriptive standard, with a tendency toward micro-managing. Besides the cost v. value equation, which did not quite seem to fit with the university mission, one of the university vice presidents added, "The state seems to think that rules and procedures solve every problem, despite much evidence that effective solutions are situation specific [122]." Comparisons were made to the SOL (Standard of Learning) exams and Virginia's new information technology project management regulations to illustrate what could happen in the security arena. "Most people in higher ed. don't want such a rigid standard," added March [123].

Carroll Trask, from the Department of Homeland Security, made the observation that standards assume the static nature of a physical environment, while cyber threats are unpredictable. "Regulation will not be very effective. You can try to be prescriptive, but can't really say 'how to' with information security [124]." Dobrosky, on the other hand, was of the opinion that the Department of Homeland Security would set standards on how to collect, identify, and store critical infrastructure information. In anticipation of the DHS (Department of Homeland Security) using the NIST (National Institute of Science and Technology) standard, the state has already begun using this standard for contingency

plans and, because of the fact that the state is made up of agencies with varied sizes and missions, they have chosen a very broad standard with best practice components, which the individual agencies will implement [125].

Trish Franklin nodded in agreement and added, "We have to make sure to address what the state policy wants in our local policy. But, every policy is different. Virginia Tech follows the same orders I follow. If you are not a state agency, you may have to follow some federal guidelines. You have to look at all policies in terms of the bottom line and meeting your audits [126]." Going on to indicate that the DHS (Department of Homeland Security) imposing standards was not necessarily a bad idea, Dobrosky also felt that the state needed to move ahead. "We can't wait two years for DHS to get their act together [127]." Describing the auditing as the state's oversight function for security policy and procedure, he went on to explain that the standard, developed in the executive branch of state government, is mandatory for every executive branch agency, which includes higher education. The internal agency auditors and the APA (Auditor of Public Accounts), equivalent to the GAO (General Accounting Office) on the federal level, take the standard and measure how each of the thirteen components is implemented [128].

These thirteen components include: *Business Analysis and Risk Assessment; Security Awareness; Technical Training; Technical Communications; Authentication, Authorization, and Encryption; Data Security; Systems Interoperability Security; Physical Security; Personnel Security; Threat Detection; Security Tool Kit; Incident Handling; Monitoring and Controlling System Activities* [129].

Acknowledging that security is a big issue, Dr. March added that, in reference to an approach to audits and public perception, use/abuse policy, which was defined as focusing on what you want to do rather than how you are going to do it, is really more relevant to the general population [130]. Using response to digital copyright violations as an example, she went on to say that working on responsible use security policy and implementation of the standards, you have to be constantly mindful of the privacy piece. "To achieve our 'safe harbor' we have to act very quickly when we receive a letter from the entertainment industry indicating that our computers have been used for illegal downloading of copyrighted material. In setting up databases and tracking this, we have to think about privacy and consider what would happen if these records were subpoenaed. Would the records contain more than we'd feel comfortable revealing [131]?"

Leonard Dalton wondered out loud how an organization could be expected to define standards when an industry has trouble doing it and Karen March responded, "Many of the network people and system administrators feel like we're not moving fast enough. My biggest beef with the State, though, is that they do not understand the cultural and political aspects of successful change management [132]." Arnold Madden, who had recently left the university environment to work in a non-profit organization, reiterated what had been said earlier, describing his current organization as more of a corporate model. "This is a very controlled environment and it is inflexible and inconvenient, but it minimizes problems," he said [133]. Madden then gave us something else to think about by seeming to question whether having a policy was always beneficial. Dr. Posner quickly responded to the new direction the conversation seemed to be taking by adding, "A privacy

policy is a statement of intention, but unless the security mechanisms are in place, they don't have the capability of living up to their promise [134]."

"From my legal perspective," Madden responded, "It's better not to have a policy than to have one we cannot deliver on. What are the legal ramifications of a policy? If you have a policy about a firewall and someone is lax about updating the software, have you created a new liability? This should make lawyers nervous…also presidents, administrators, and IT officers. A policy can be used against you. The reason for having a policy is to alleviate risk. Right now many schools are doing risk assessment or analysis or paying someone else to do it. But, if you are going to identify problems, you may be creating another problem or liability. There is a give and take, a balance. This should be approached holistically [135]."

Lois noticed that, while there appeared to be numerous laws and standards with regard to dissemination of information, participants pointed out that prescriptive standards didn't fit well in the university setting and also noted that actions taken to comply with them conflicted with what some of them saw as larger concerns, referring to "Big Brother" and invasion of privacy. In discussion of information security, it is common to hear talk about responding to threats and several panelists now spoke about how they see the role of security changing. "In regard to Homeland Security;" Carroll Trask began, "under the guise of academic freedom, we may have foreign students who have access. In general, we like to think they do not have evil in their hearts." He went on to point out that there are those who exploit the honesty policy of the university and went on to use several examples to illustrate his point. Irrigation is a problem in São Paolo and Rio de Janeiro and Brazil

sends lots of engineering students to U.S. universities. We feel fine if they are accessing the information while they are here, so what is the problem with their doing it electronically?" The problem, according to Trask, is that one of the ways to spread germ warfare is through irrigation and water supply systems and that by allowing open access to these systems, we are running that risk. "A hacker got into the system that controls a dam in Colorado," he added. "He was not trying to do damage and did not take control, but if he had, this could have done more damage than two nuclear bombs." Trask went on to cite another similar case of cyber terrorism involving a waste treatment plant. "There are people who exploit the honesty policy of the university. A crude example is that nineteen of the hijackers were students (referring to 9/11). They took advantage of our 'freedom' and scarred our psyche [136]."

"As we've started to benchmark, in the corporate world," commented Arnold Madden, "it's become apparent that, post-9/11, information security has become a sub-set of public safety or physical security. We think higher education will evolve to this, as well [137]." Trask agreed, "The assumption of a threat is built into risk assessment. Everything is vulnerable. We found that out in 9/11. Who would have thought that our own planes would be a threat [138]?" Participants from the community college agreed with those from the university who remarked that there was now a push for security to become a bigger piece of what they do. Dalton acknowledged that most schools now have at least one full-time person responsible for security and Dr. Thompson pointed out that in many institutions, IT has gone from being a capital expenditure to being an operating expenditure. Whereas payroll would have been considered the most critical in the past,

that has now been replaced by communication systems. "In 9/11 communication broke down. Even at the university, there was a great surge in voice communication [139]." In addition to a greater emphasis on security awareness, 9/11 was seen to have contributed to people thinking differently and broadening the scope of security and thinking about critical assets [140].

Madden noted that, in his experience, universities can tend to focus on physical events or emergencies, when developing emergency preparedness plans and pointed out that terrorist threats can also involve cyber-terrorism and we needed to make sure it wasn't left out. "We need to think more inclusively about groups that are impacted [141]." Trask supported this by reminding us that Dick Clarke's reason for resigning as cyber-security officer for the Bush administration was a result of his feeling that the current administration was not taking cyber-security seriously enough [142]. Information security threats included Microsoft system vulnerability, the lag time between the threat and development of a patch, DOS (Denial of Service) attacks, viruses, virus maker web-sites, Trojan horses, pranks and hackers, data protection, computer hijacking, spy ware, dangers of peer to peer file sharing, identity theft, and illegal downloading [143]. "It's interesting. In my policy role," said Madden, "I've become aware of all kinds of security issues that are a result of misuse or misbehavior: harassment, stalking, SPAM, or mass e-mail. Copyright violations go in this category. These are not technology problems. They are security issues [144]." Rick Smith added, "There are esoteric kinds of things to consider in policy development," mentioning identity theft and fraud, in particular [145].

"Once someone's computer is hijacked and used to download files or for some other activity without the user's knowledge," Madden informed us, "the incident goes from being a technology issue to a security issue [146]. Karen March agreed, "It's like someone stealing your car to rob the 7-Eleven [147]." Incidents related by both university and community college panelists included the hijacking of a computer at Virginia Tech on November 3, 2000 with which hackers then changed numeric elements associated with the IP (Internet Protocol) address so that anyone accessing, Yankees.com, the New York Yankees web-site, would view pornographic materials that had been installed on the Virginia Tech Computer; and one where a student who had installed a mini-camera on his computer to use while chatting with friends, which was then used to spy on him in his room when someone took over his computer [148].

Dr. March then adapted the 7- Eleven scenario to illustrate problems with peer to peer file sharing. "If I lend my colleague a password and he or she uses that password to publish something, we are both liable," she said. "It's like lending someone a car to rob the 7-Eleven. You didn't rob the store, but you helped that to happen [149]." "Do you remember the Columbine incident?" Dr. Bailey asked. "After that occurred, I realized that we have a vulnerability just by giving someone locker space and letting them put a lock on it. It could be a bomb." The open locker policy at our school has now changed and students now sign up to use a locker with a school lock and agree to random inspections of the lockers. "I've thought of it. Someone else might too," the president added [150]. With regard to information security threats, specifically, Trask mentioned SCADA (Supervisory Control and Data Acquisition) systems control. "Just think what kind of

damage could be done," he said, "if someone made all the traffic lights green at rush hour [151]."

Invasions of privacy, resulting from data aggregation, data miners, as well as personal information stored in government and private sector databases was of concern to some [152]. "Most Americans seem much more comfortable with the private sector having personal information than they do with the government. I feel just the opposite," said John Ripley [153]. "Another concern is invasion of privacy with increasing levels of security," added Trent, "I like AOL, for instance, but I don't like that they can read my instant messages. That feels like 'Big Brother.' I like it that they can lock down my e-mail if someone hacks in and starts sending messages our from my e-mail account. In that case, it feels good to be protected [154]." Brad Martin expressed concern over the Patriot Act. "There is a lot of technology alluded to in the Patriot Act, wiretapping, etc. making it easier for the government to use new technologies to invade privacy," he said [155]. "The guiding principle should be that we do everything possible to preserve individual freedom," Matthew Barnes added, "Instead, what I see, under the rubric of security, not data security, but Homeland Security, the sort of things that are stated demonstrate lazy thinking. For example, since 9/11, there's been an emphasis on security, not only at the expense of privacy, but there is also this appearance of focusing on security when things aren't really improving [156]."

It was clear that our panel had more to say on the privacy issue, but it was time to break for lunch and Lois suspected they would get the opportunity in one of the later programs, so this was probably just as well. On her way to lunch, Lois considered what

she'd heard about threats. Whereas, earlier we'd heard the advantages of an open system that discloses it failures for improving security, this afternoon, we'd heard that this kind of system put us at risk of computer hijacking and was being looked at differently in the corporate world post 9/11, as information security policy reflects more of a public safety focus. While this focus included attention to cyber-terrorism, some also talked about making broader connections to security, in general and issued warnings about practices like peer to peer file sharing that could result in liability for higher education institutions. At the same time, concerns about information sharing and the compiling of databases were seen as threats to individual privacy. As policy is developed to respond to these varied threats, Lois thought, it will be interesting to hear how policy alternatives are discussed. As she sat down to eat, she was already looking forward to the next program on language and framing in policy development.

Program #3: ***Language and Framing in Public Policy Development***

As Lois waited for the rest of the panelists to return from lunch, she was excited to hear people beginning to engage in some discussion about the next topic. As she glanced around the room, she picked up on some snippets of conversation, "You'll have to understand that what I say is framed within my understanding from an educational standpoint," said Roger Trent. "Mine is the voice of public policy in all this," commented Dr. Martinez. "With a background in materials science, I came into government with a much broader view," added Trask. "I'm not a technologist, I'm an English major," Alice Thompson informed them. "They hired me as a translator. [157]"

This was exciting. Just as Lois was about to sit down, Carroll Trask, from Homeland Security, came up to her and complimented her on the program. "These are important questions," he remarked. "We should be discussing these issues in think tanks [158]." After all her hard work, this made Lois feel great. She introduced the afternoon's program with enthusiasm and sat down to listen and learn what our participants had to say about language and framing in relation to policy development.

Mitchell Posner had a thoughtful expression as he started things off. "Framing…the way in which you frame issues should be factual driven. It's hard to generalize [159]." "Framing does play a part in policy development," added Roger Trent. "Knowing that you need to get people to buy in will influence how you frame an issue. For example, if you say that there's been a report that Sadam Hussein is on a plane and is on his way to New York with a bomb, panic might result. However, if you start by saying, 'Suppose we consider this scenario…,' the result will be different [160]."

Karen March explained how her university had used their audit as an opportunity to make a real difference in security. "Rather than assuming that the central IT unit would have sole responsibility for information security," she added "recommendations to the auditor's findings were written to involve a high level of executive involvement." By doing this, Dr. March was able to assure the cooperation of the deans necessary for the plan to succeed. "This is an example of framing," she smiled [161]. "Framing is the purpose or rationale behind a policy," explained Arnold Madden "and sets the context for ensuing policies and procedures [162]." "Framing would be different for an international emergency or for a local emergency," added Roger Trent. "If I want to sound intelligent,"

Carroll Trask candidly revealed, “I’ll frame a question so that I know I can give a competent answer [163].”

“One should choose framers and words carefully,” Dr. Thompson added. “In framing the constitution, our forefathers didn’t assume broad participation. I wonder how you get that [164]?” “In stable times, we used to talk about *education*,” she added. “Now we talk about *lifelong learning*. *Education* was a more stable construct for more stable times [165].” Dr. March commented, “Even if we think about technology, the answers to the questions we’re considering will be different, depending upon whether we’re considering individual citizen data or enterprise data.” “And your perspective,” added Roger Trent, “Homeland Security, for example; sitting on the Governor’s Cabinet, I’m involved with decisions about which buildings to close or who gets protected. It has to do with a level of responsibility. My perspective is very different from the one I’d have if I were just thinking of protecting myself and my family [166].”

“Who gets to frame the issue also can make a big difference,” added Sophia Martinez [167].” Bob Moseley, our private sector security solutions panelist agreed, “In policy making, power is important. That’s very true with security [168].” Rick Smith, counsel to the House sub-committee went even further. “The framing really **is** the policy,” he said, “look at the way the Republicans have usurped what had been thought of as a Democratic issue, the Medicare Prescription Policy, and framed it as a benefit for seniors. Democrats think the Republicans have ruined Medicare. You can go on and on about the effects of a policy, but the policy itself cannot really be separated from the framing [169].”

"Are you familiar with HIPAA (Health Insurance Portability and Accountability Act)?" asked Moseley. "In this organization it is with the health guys. It is framed as a health issue because it has to do with medical records. The information security guys are lesser players and the physical security guys even more so. The responsibility is with the health solutions guys out in San Diego. They could have called this an information security problem. One reason they didn't was that the information security guys were not in the hospital. They didn't have the contacts [170]."

Karen March spoke of security as an emotional issue, "I have to re-write some of the policy drafted in my unit. Residence Hall students are not the enemy. They are victims as much as anything else. If you frame policy in a combative way, it will not make it through the layers it will have to go through to be approved [171]."

Sophia Martinez agreed with what some others had said about the importance of power in framing and used Homeland Security as an example. "Framing was going on when relevant institutions were listed, such as FBI, CIA, and Immigration. There was actually a debate within the Coast Guard. They didn't want to be re-defined by Homeland Security's pulling them into law enforcement. They reminded us that it was important for them to remain neutral, in a sense, and be available to help people floating off the shores of the US, etc. A redefinition could mean that they lose some of their multiple roles [172]." Posner also had something to say on this and indicated that these different government agencies would have views that differed from each other, but that they were all players along with those on Capitol Hill, the House, the Senate, the different political parties, consumer groups, and those who look out for civil rights and the impact of technology on

our lives [173]. Martinez then said a few words about threats and how the issues are currently being framed. "In the security area, military, technical, hardware types define the threat as something coming from the outside that is going to get you. I'd like to see it in a larger context. What kind of community do you want [174]?"

While Ripley agreed that some players do have more power, he pointed out that this does not give them a monopoly on the debate. "Even with the broad participation allowed by the Internet," he said, "at the end of the day, for the US and most other countries, the policy process is well articulated and well identified. At the core you have the White House, leadership of agencies, and Congress [175]." Bob Moseley took this opportunity to demonstrate how framing could be used to exclude players from the discussion, "As to the question of power, me, as a physical security guy…if a question is framed as strictly IT (information technology), they could exclude me from the discussion, claiming it is "information security only." They would take ownership and funding to apply where they think it is the most important. Of course, it could work the other way too [176]." Carroll Trask agreed that framing was important, but also added, "The other side of the coin is who the policy maker surrounds himself with [177]." The concern here, Lois surmised, was that, rather than seek out alternative perspectives, policy makers would either take the advice of the people they'd surrounded themselves with or look to paid lobbyists to frame the issues. Matthew Barnes gave an example, "What we see is excess attention paid on telecommunications and technology policy that favors business interests at the expense of individuals and smaller organizations [178]." "And the press," added Ripley, "In terms of framing, analysts thinking about new sources of risk got into the

public media and got White House attention. If it's on the cover of *Time Magazine*, it's going to get attention [179]."

"With regard to framing and the White House," added Brad Martin, "I think you have to give credit to the Bush administration. They get an A on its ability to frame policy since September 11th. Early on, they used all the right words and pushed all the right buttons that made the road to the Homeland Security laws and policies a very easy one to travel. They had the luxury of the time…the buttons were easier to push. When you look at the people in the administration, from George Bush to John Ashcroft, these kinds of proposals were already on their agenda before September 11th. They were opportunists. Even those who do not like anything else about the Bush administration give them credit for framing policy [180]."

Lydia Johnson remarked that one of the ways she could relate to this discussion of framing was by being cynical and asking, "How can I spin this [181]?" Karen March spoke of how she'd made use of what she'd read in a book on technology marketing, "It talked about different categories of people and the level of acceptance of change." She went on to explain how this approach had been useful to her in getting buy-in for safety awareness. "Not one presentation was like another," she said. Focusing on getting administration to buy in first, March confided, "The vice president was pretty savvy. The provost was not." With the provost, she'd talked about the impact on the people who work for him; whereas, with the vice president she focused on the image of the university, compliance issues, and things related to poor management of security and accountability [182]. While recognizing the importance of getting the support of administration first,

March added that, in speaking with faculty, “I didn’t bring this up if I didn’t have to. I didn’t want to use it as a hammer [183].” “If you are asking faculty and staff to be on a security committee,” Arnold Madden added, “they may view this as something that might be restrictive or tighten things up. However, it is also important for availability. I’d emphasize that you need to have your computer available to do your work and it needs to be protected from viruses or other dangers [184].” In applying this to government, Carroll Trask noted, “It’s easier to be a hero than a preventer, though,” Trask added. “If you prevent something, then nothing happens. There’s no evidence. How do you measure that? You can get jazzed up about the response side. You’re a hero and you get appropriations [185].”

“Framing is putting things into context and how one should think about an issue,” said Rick Smith [186]. For example, a strategic context such as Democrat/ Republican or security of electronic information and security of a document. “What if you put *secret* or *top secret* on a piece of information; then you have standards. On the other had, a designation like *confidential* really needs to be considered in context [187].” Karen March added, “Policy developed within a vacuum, without considering the context is meaningless [188].” Mike Dobrosky agreed, “Framing predefines and sets boundaries around the issue. For example, I might see an issue as predominantly a security issue, but recognize that it has some aspects related to Freedom of Information. Someone else might say that a constitutional right trumps security and that this needs to be framed as a Freedom of Information issue [189].”

Dr. Martinez commented that she'd like to see security considered in a larger context. "Maybe we could lower risk by things like improved international relations [190]." Dr. Thompson made reference to Donald Schön, who wrote about the reflective practitioner. "You have to have time to reflect. He was talking about the academy. I think it's larger than that [191]." Trask compared policy making in government to strategy in business. "In business," he continued, "policy is what we are trying to achieve or setting the mission. Government really needs to look at the threats, vulnerabilities, and consequences. Otherwise, security is just a deep, black hole into which you can throw dollars ad nauseam, ad infinitum [192]." Dalton, on the other hand, expressed some optimism, "The CIOs (Chief Information Officers) of today seemed to have a better grasp of both technology and business processes. As things change, it's important to have this knowledge of the functional side [193]."

"Good policy is developed by unpacking the problem. I don't see this being done today," Trask sounded disillusioned. "The pace is so fast," he continued, "People tend to grab at the solution first and then figure out how to implement without going back to the problem. It's a waste of resources. It's a good thing we are a wealthy country. So much depends on luck. Working on policy is fun and really interesting, but kind of like making hash. I'm an operational person who came to work to government to work on policy. Now I'm considered a strategic thinker [194]." Carroll Trask continued, "Careful thinking and analysis make policy stronger. So do strong opposing views and deliberation. In the Reagan years, the best policy out of the National Security Council resulted from those with strong opposing views who were encouraged to air them openly. That caused proper

balancing. The worst policy is developed when one strong person always gets his way. Policy is understanding trade-offs, making choices, recognizing consequences and managing those consequences [195]."

Lydia Johnson commented, "Policymakers tend to do things in terms of their own vested interests [196]." "The way policy gets made is damaged," agreed Trask [197]. Johnson went on to use higher education to illustrate what she saw as part of the problem, "While management is concerned with doing things right, leadership is concerned with doing the right things [198]." You have to start with the end in mind. What does it look like when it's done? What does it take to get there [199]?" added Trask, "Policy recommendations for security were all over the map." "You need to think systematically," he added. "Whether or not you come down on a particular side for political reasons, you still have to have analysis. If you don't have proper discipline framing, you end up with bad policy and really bad implementation [200]."

"I've found one problem solving technique that involves enlarging the boundaries in order to lead to a better solution," Dobrosky added. It may be easier to get at root causes or bring other solutions to bear. Very often, rather than making the frame smaller, it works better to make it larger [201]." "What is the policy question?" Lydia Johnson interjected. "Policy-makers sometimes ask the wrong questions," Trask added. "Encryption policy, for example, resulted from poor policy decisions. "No one thought that through or asked the right question, "What are the consequences?" Now we're playing catch-up. It's the same thing with the economic situation, going off-shore. We now have supply chain problems in terms of national security. This occurs when there is

no holistic view. If you're a systems thinker, you go where you need to go. Here there is turf and territory [202]."

"Issues may be framed by the Governor or the legislature," added Roger Trent. Dobrosky agreed adding, "Conflicting legislation, such as the Freedom of Information Act and laws that compel us to secure information and keep it from public view are related to framing. For example, we've been directed by the legislature to deal with security of web access to circuit court records and in such a way that we have to know who has access. That was the legislative charge. There are a number of people who say that court records contain information that should be kept private, such as social security numbers or mother's maiden name and want to restrict those data elements. Because they define the problem differently, they don't think we're doing our job [203]."

Then again, by limiting focus to something like data elements, Lois thought, you run the risk of having that interpreted in purely technical terms and distracting from the big picture. Dr. Johnson seemed to echo her thoughts "On this project I'm working on, I was presented with five different surveys proposed by the community college system. They contained so many acronyms that the end-user wouldn't have had a clue [204]." "People don't always know how to ask the right question," she added. "It's important to bring in someone who can understand both sides of the conversation," contributed Leonard Dalton [205].

"There are mechanisms for translating concepts into policy," added Ripley. "It's important to understand the process and work it in. The Internet culture, at its heyday, often proclaimed, 'government just doesn't get it', but you have to be part of the dialog to

influence policy. You can either explain the issue or have Washington go ahead and squash you. Policy really needs to be written in a way that can overlay technology. Congress does tend to have a hard time dealing with new technologies, but this is more of a conceptual problem than a language problem. There isn't a good model for thinking about policy for new technology [206]."

Alice Thompson pointed out that, in speaking of quantitative measures, numbers are abstractions, just as words are, "We've created technologies and we interact with them and we need to understand this interaction." She also noted, with reference to framing, if, when we are developing policy, our language is one of controls or master cylinders, the policy might be very different that if we were to use another metaphor, like the shepherd and his flock [207]. "At one time, the medical profession used metaphors of control for the brain or for the heart," she continued, "but it's not one organ. The organs of the body have to work together. How we frame policies related to information and security is very important. We could end up with hierarchies and controls again. I hate what is going on with our language. We're a super power, responsible for the world. We're not talking about things like sharing. We're talking as if we can save the world with force and we will set the terms [208]."

"Language can be a barrier," Dalton added in reference to complicated privacy statements and jargon that can be useful shorthand to those who understand it, it is of no use to those who do not. "Most people who use applications," added Lydia Johnson, "don't actually need to know the details of how they work [209]."

In regard to infrastructure, Dr. Thompson saw Congress as making decisions about infrastructure without content and about content without infrastructure. "They have little understanding of the language of zeroes and ones that inform infrastructure or content development today [210]. From Rick Smith's perspective, language was not the central issue. "You can come to agreement on language and what it means. Debate is over implications. For example, how well does the average person understand the tax codes [211]?" Brad Martin did have some concerns about language and referred to the state commission that proposes laws related to technology, "When you go to their meetings, you get the sense that two languages are being spoken and that very few people seem to speak both. It worries me. What kind of policy gets made in the Tower of Babel [212]?"

"There are many technological languages," added Carroll Trask, "Coming from private industry, I found that I spent half my time explaining myself to others and the other half trying to figure out what they were saying to me [213]." Sophia Martinez claimed, "Technologists seem to feel that policy people are hopelessly inadequate in speaking about all this [214]." Thompson, however, spoke of numerical literacy. "If you're not familiar with the language of zeroes and ones, you abdicate your ability to behave in an informed way in a technology-enabled environment [215]." Mike Dobrosky seemed to find this particular discussion especially interesting and talked about his own agency, "Language is absolutely essential. In this agency we've talked in terms of the need to develop a common language. We've been set up to make technology a utility, just like when you flip the switch and get electricity. We've been told to bring in ninety-two agencies to make up this one. A language that is a best practice will help us to achieve a commonality of

understanding and purpose [216]." Mitchell Posner showed how this might be done by defining elements and mechanisms, "*Integrity* means that security is what you expect it to be, *privacy* is your intention, and *security* is your capability [217]." Dobrosky added, "For the most part, technological language consists of fairly standard words that are put in a different context." While acknowledging that this is not very helpful if you don't know the language, he also pointed out that there are times when we need to make the effort to translate to include people in the conversation and that there are other times when, to be part of the conversation, one must learn the language [218].

Dr. March spoke about this in relation to the IT unit at her university. "It's difficult for highly technical people in my unit to write warning notices. They say things like, "We are in danger of an RPC exploit." I don't even know what that means and my degrees are in computer science. Right now, I am establishing a position to hire someone who can communicate with ordinary people about technical issues. If we're going to educate the university community, we have to translate the jargon into language people understand and organize the discussion so the executives who approve policy understand what we are saying [219]."

"From outside the technology arena, there is clearly a language problem," Martin added. "My concern about the language is that we run a risk of creating a language that is so rarified that policies become incomprehensible to the vast majority of people. And when policies can't be understood, our natural distrust of government is exacerbated. This can also create a situation of haves and have-nots with half the people understanding language about new technologies and others having no idea what it means. This might be

an intellectual schism or an economic schism. It excludes a lot of people, not just from influencing policy, but from understanding it [220]."

At the same time participants agreed that policy had to be in language that people understand, they realized that there is a need to be precise. Mitchell Posner proposed that one way to handle this is to have the policy written in English and the standards and procedures in technical terminology [221]. "It's amazing how loosey-goosey people were with terms that have very specific meanings," Trask added. "Sometimes conclusions are drawn from inconsistent language," Dalton pointed out. "In some respects, new languages are being developed," added Alice Thompson. [222].

On the question of whether technological language should be used in policy writing, some thought that, if the policy is a technical one, this is appropriate. "Is this an information technology policy or an information security policy? Depending on what you decide, you'll go down two different paths," said Arnold Madden [223]. Dr. March spoke of use/abuse policy, which focuses on what the policy is to accomplish, rather than on how it is to be done and also examples of laws and policies that have been written around technology. The way the FCC treats telephone and cable providers and differences in legal recourse between manual and on-line data entry were mentioned as examples. "They are each treated entirely differently even though they are offering the same service. It's absurd. The FCC is trying too hard to regulate specific delivery systems rather than focusing on access generally and how bytes are delivered. Nobody cares what transport mechanism is used," said Matthew Barnes [224].

"The more important issue, though, is framing," commented Posner. "Those who are successful are those who can explain complex things in simple terms. You frame the issue and put them into English. I tell people to talk to me as if you're talking to a high school student. Explain complex things in a simple way [225]." He suggested that simplified English be used in privacy policies [226]. Karen March brought up the issue writing policy based on a specific incident and described it as failed framing. "What happens is that you don't recognize the next wrinkle and the policy is useless unless an identical episode occurs." The other problem is that very technically specific policy will be outdated immediately," she added [227]. Roger Trent explained how *scoping* can be useful. "Scoping, or taking your audience into consideration, affects how policy is written and developed, as well as how prescriptive it might be [228]." Karen March added that, when she came to the university about ten years ago, most policy in her unit was written to be interpreted by technical personnel. "For the first four or five years, I didn't write much policy. I spent my time interpreting existing policy to see where the pieces fit." She found that there were already disciplinary mechanisms in place for students, faculty, and staff [229]. She went on to discuss use/abuse policy in more detail, explaining that she defined security broadly and that technologically specific policies often do not need to be written, as there are already existing policies under which incidents may fall. "This is a result of technologists writing policy instead of 'big picture' people [230]." Using the example of FERPA (Family Education Rights and Privacy Act) defining directory information, she pointed, "Another advantage of use/abuse policy over technical policy is that it does not need to be re-written so often [231]."

Mention of FERPA brought some criticism from Leonard Dalton, who claimed that the problem with FERPA is that it was written with paper documents in mind and that it was twenty years out of date [232]. Trask pointed out that they were both actually saying the same thing in two different ways. "Good policy is hard to write. It can take twelve to eighteen months and you can end up with a benchmark that is useless if you write with a specific technology in mind [233]." Karen March explained why use/abuse policy is preferable, "A technical policy might say that you have to put up a firewall. Firewalls that keep out ninety-five percent of nefarious activity is an objective you can measure, but another way is to block specific ports. You may be able to say that you are complying by keeping out ninety-five percent of the activity, but something could be coming through on another port that you have ignored [234]." Trask added, "Don't focus on 'how to,' but on 'what' needs to be done. In your home security policy, for instance, you might say, 'People who want to harm me can't come in.' If you become overly technical, you might try to list all the possible weapons someone might bring, but forget to include knives. They could enter with a knife and still comply with the policy [235].

Mike Dobrosky informed us, "The state's standard says that the agency head is responsible for the information in their agency and so is a stakeholder [236]." Others pointed out that, while this may be true, they were not the only stakeholders and others were listed. "Everybody is really a stakeholder in information security policy; getting a drivers' license in Virginia, for example, the 9/11 hijackers were said to have obtained ID in Virginia. When that rebounds, we go to the other extreme and everyone is harmed who would have used that service [237]." Mitchell Posner made the point that the interests of

individuals need to be taken into account. However, whether they know about it or have much say is sometimes not the case. "Virginia has the strongest anti-SPAM law. I don't know whether all of the stakeholders had much to say," he said [238].

Lois noted that, in discussions of security, participants continued to voice a number of varying meanings and definitions. Arnold Madden, who'd worked with the university and staff from Homeland Security made a distinction between *security* and *assurance*. "Security has to do, specifically, with assurance and cyber-security [239]." Further distinctions were made between physical security and non-physical security and what components make up security. "The concept of security involves two things: having permission to access some entity and assuming responsibility," said March [240]. Others talked about protecting assets, protecting data, feeling safe, safeguarding classified or confidential or critical information, and protecting networks and systems. Security was also described as a requirement. "We talk about the iron triangle. It consists of time, budget, and quality," said Mitchell Posner, "We usually say, 'Give me two out of three.' Security is in the mix. It's a trade-off," he continued [241]. While Bailey, Trent, and Martin reminded us that security can include things like a healthy environment, a financial nest-egg, and protection of freedoms, Trask added, "The whole area of security is very ill-defined, particularly in information security. The definition of security needs to be unpacked." He went on to say that there was an analytical process involved in this and that people really had not done this [242]. "Security can mean many different things," interjected Posner, "Traditionally, we think of defense, people feeling safe in their homes, geopolitical security. We have international, national, state, and local views of people

being secure in their homes and in the world [243]." Public safety, national security, network security and national security issues were, at times, confused, as were technology and security issues. "When you talk to some people, they speak from a defense perspective," Posner added [244]."

This part of the program was absolutely mind-boggling. Lois continued to hear security defined. There was geopolitical, international, national, state, and local security. She heard about security clearance, physical, mental, and spiritual security. There was security of the document, securities, in terms of stocks, and more. "Security is in the eye of the beholder," Bob Moseley summed up [245]. Posner agreed, "For this reason, it is important to define what you mean by security when using a catch-all, especially since 9/11 to the extent that people can find a way of talking about certain types of security. The Eskimos, for instance, had many different words for snow. Prior to 9/11, the term Homeland Security was not part of our mind-set. This event has changed the way we speak about things. I don't feel satisfied with discussions surrounding security [246]"

"One thing about HSPD (Homeland Security Presidential Directive)," said Trask, "They define things up the wazoo! Presidential documents have to have very accurate definitions. I wish everyone would do that [247]." In addition to recognizing that there is confusion about the meaning of security, the importance of being able to understand the big picture was mentioned, as well as the need to be careful in our conversations about security. "Security becomes a way to justify what somebody wants," Moseley commented, as he described how, as a member of NDIA (National Defense Industrial Association), he'd found himself moved to the Homeland Security section. "Our customers are

different. We work with different people, but they wanted to put us in that section because it had the word "security" in it [248].

As the time for discussion was coming to a close, both Brad Martin and Rick Smith had something to say. "Today, security is a buzz word for a more empowered government, moving us toward something like a military state. 'Security' wouldn't have had these connotations a couple of years ago [249]." "According to General Ashcroft, I should feel more secure if he's more powerful," added Smith. "I'm not sure an Ashcroft dictated security policy is any better than Hussein. One is a little less severe. It's like pregnancy; it's hard to be a little or less pregnant [250]."

Lois had suspected that the language people used both reflected and influenced their perspectives in that technical terminology, focusing on the processes of how technology works could, when used to frame information, might result in policy that did not incorporate larger issues. However, the discussion she had just heard seemed to be even more complex. This did not seem to be merely a matter of focusing narrowly, but of a constant shifting of position and frame of reference in what appeared to be a way of making things fit. Lois realized that she had expected varying perspectives among the major stakeholders. But, it seemed she'd expected clearer boundaries to be drawn and interaction to be in some predictable pattern. Words like language, framing, perspective, context all figured prominently in what appeared to be a search for a way to communicate about an ever changing phenomenon. How do you make policy in this environment? Are we dependent upon definitions frozen in time or are effective policy decisions dependent upon the ability to continually take in and synthesize new information? In the next

program, we would be considering public policy with regard to security and individual liberties and whether trade-offs were necessary. While Lois anticipated a lively and interesting discussion, she was beginning to realize that the more she heard, the more complicated things got. She remembered a quotation by F. Scott Fitzgerald to the effect that the mark of a true intellect is to be able to hold two opposing views in one's mind at the same time and still be able to function. Lois smiled as she realized that this probably was, at best, a minimum requirement for thinking about all this.

Program #4: Security, Individual Liberties, and Public Policy: Issues of Trade-off

Panelists had touched on the issues of individual liberties and trade-offs in some of their earlier programs and Lois Lassiter looked forward to this final discussion in the series as one that would, undoubtedly be thought provoking. As she made her way across Virginia Tech's drill field and headed for the large stone building, which would house this last program, she started to realize that she was eager to hear what her guests had to say and that, while an irrefutable understanding of the complexities of the context of information security policy she'd been studying all these months was, undoubtedly, out of reach, she was more than satisfied with this opportunity to attempt to come a little closer to it. This was on Lois's mind as she introduced Secretary for Technology Strategy and Planning, Mike Dobrosky, who would begin today's discussion, "It has been suggested that there are necessary trade-offs between individual freedoms and security. Would you talk some about this?" she asked.

"Trade-offs; yes, I think they're inevitable," Dobrosky began. "Your freedom of expression ends at the tip of my nose [251]." Trish Franklin agreed, "Yes, there are trade-

offs. Do you want the security or do you want the freedom to do what you want to do [252]?" "Well, I strongly resist the notion that you can have trade-offs of such sacred values," Rick Smith interrupted, "I would like to be part of a conversation that maximizes both. By agreeing that trade-offs are necessary, we accomplish, for those who would wish us harm, what they could not accomplish by themselves [253]." Dr. Thompson and Dr. March agreed that in any community, there must be some compromise for people to live and conduct their affairs, but Dr. Martinez emphasized the importance of talking about these issues. "I am trying to put together a data base of security/ policy level organizational kinds of things that address security such as HIPAA law and the Patriot Act. I'm looking for patterns that will help us to discuss the bigger picture. How can we talk about some of these concepts in the language used by those involved in the inner workings of computer security [254]?"

Bob Moseley focused on the importance of technology in helping to alleviate the trade-offs. "The elevation in the need for security drives technology to find ways to mitigate intrusion to individual freedom. Right now, it's pretty painful if you travel much, like I do. Technology is not there yet. What needs to happen is that technology needs to move on to mitigate the loss [255]" Brad Martin, on the other hand, felt the capabilities of technology make personal security somewhat difficult. "There is a significant erosion of privacy for the sake of security," he said. Citing the ease of use of cameras for increasing surveillance, he added, "The development of new technology combined with the broader authority of the Patriot Act to use it is one of the most frightening aspects of the policy changes taking place right now [256]."

Carroll Trask, from the Department of Homeland Security, spoke about technology, policy, and people as the "three legs of security." "Even with the most secure telephone lines and encryption," he said, "any one of these three legs can fail. You still must rely on voice recognition and make a judgment call that the person on the phone is who he says he is [257]." "One concern with increased technological surveillance, though," Martin added, "is that people don't always know about technology or have an immediate sense of having lost something. What do you lose with these erosions of privacy?" A lot of people don't care. That has to be one of the difficulties [258]." Sophia Martinez agreed, "Sometimes it seems like a hopeless quest. How can we bring this into a democratic dialog when people don't want to discuss it or think about it? Who really understands that this is not a good trade-off?" She went on to note that, in addition to their being no real public dialog, political scientists also seemed to be strangely silent [259]. Brad Martin agreed, "One thing about the ACLU (American Civil Liberties Union) is that, to a certain extent, they've gone through a transformation since September 11th. What happened right after that date was that many of the groups that advocate for issues such as privacy and free speech really stopped talking. The ACLU was one of the few groups that didn't become silent. Since 9/11, as concerns grow, people are looking to them for public education. Before this public education was something ancillary to what they do [260]."

Karen March pointed out that, within the technological realm of information security, there were trade-offs because it was required that standards be set and observed. "Security does constrain individual freedom, just as civilization does," she said [261]. Brad Martin added, "The government should restrict freedom only when absolutely

necessary [262]." March replied that you really had to be mindful of both, "When security is really needed, you have to think about privacy of the whole university not just the individual [263]." Another issue, Brad Martin, noted was the loss of "functional privacy." "Information that has always been essentially private because of its inaccessibility in court houses," he pointed out, "is now available on the Internet [264]." Karen March felt that identity theft legislation would eventually result in social security numbers being purged from documents [265].

Both Brad Martin and Sophia Martinez expressed concern over due process. "Yes, my problem with the Patriot Act," said Martin, "is that usually you assume that government officials are putting policy decisions through the civil liberties filter. In November 2001, the filter was thrown out. If it had been in place, the Patriot Act would have looked very different [266]." Sophia Martinez was thinking of foreign students, in particular. "This is a big issue," she said, "The whole thing is abysmal. There is a whole different regime. This really has to do with framing too. To what degree will we extend our beliefs and values to others? This is one of those trade-offs. How do you pin this down so you can talk about it? What to do about foreign students is one of the biggest security issues for the university right now [267]."

"Maybe minorities have a better understanding of this," she added, "They may not be as trusting of that kind of power. On the margin, that kind of culture can infringe. They might have a heightened sense that there really is a trade-off [268]." Martin responded that, in his experience, the most irate callers to his agency were middle-class, white people who'd had their houses searched by accident and he gave a couple of examples involving

citizens brushing up against intrusions to liberty that they were not used to [269]. Ripley now joined the discussion, voicing the opinion that trade-offs are badly measured. "The U.K. has much more intrusive laws, but no one calls it a dictatorship and says that civil liberties are dead. Show me the trade-off. Is this really a trade-off? Other things worry me more, like the Secret Service getting crazed, closing Pennsylvania Avenue [270]." While Martin agreed that security is a necessary function of government, he didn't endorse what he saw as an "either/or" mindset. "The important thing about security and the role of government," he added, "is that security must always be seen through the prism of individual rights [271]." Several panelists from the college and university group had been to a conference, *Countering the Risk of Terrorism*. "There was a lively discussion about this issue," said Karen March, "There was a strong opinion laid out, and I believe most agreed, that there are not trade-offs. They work together. There needs to be a balance [272]." Alice Thompson referred to Kenneth Boulding, a cultural anthropologist, "He wrote in the early eighties. He puts a lot of constructs on a continuum…things like: evil, good, beauty, ugliness. None of these are absolutes. We must figure out what the good balances are [273]."

Martinez spoke at some length about what she viewed as the cynicism dominating public policy. "The academics most closely associated with security are the 'cold warriors' of old," she said. "I am an institutional/structuralist/functionalist type person and I touch it with trepidation. There are not a lot of good analogies of cold war and non-state entrepreneurial terrorism. This has allowed others to come into the dialog, but it is dominated by cynicism, geopolitics, and incrementalism. I'm ambivalent. It's kind of like

consorting with the devil. It brings you into contact with the worst instincts of humanity. In fact, the cynical types tell us, 'You idealists can't handle this.' However, the alternative is to leave it to those cynical types [274]."

Homeland Security and information sharing were also discussed. "From a political standpoint, the Department of Homeland Security was a good idea," commented Dobrosky. Dr. March added that universities were interested in sharing information on incidents, but Lydia Johnson expressed some concerns. "On the flip side is worrying about how much information people have a right to have once data are gathered," she said, "In terms of personal freedoms, how much information do policy makers and decision makers need? We sometimes collect too much information. This is a threat to freedom. But it may help identify 'bad guys.' That's a problem: how much to collect and who has access and for what purposes? What do you need to know and why? Unless you can say why, I'd see it as a threat [275]." "When statistical information is gathered," added Roger Trent, "interest is in categories of people and efforts are made to purposely not collect personal data." Leonard Dalton agreed. "If you can collect it, you can protect it," he said [276].

"With regard to information sharing, from the government's perspective, if we know where everyone is at all times, we can maintain security," added Brad Martin, describing TIA (Total Information Awareness), a proposal to compile information on individuals from a variety of sources, including medical, tax, and other government records and connect up with private sector databases to prospect for potential terrorists. "This plan was shot down," he added, "I don't really have the details. I think it cost a lot of money. It was one of the most frightening proposals [277]." Ripley disagreed and described TIA as

a proposal that did take civil liberties into consideration and was developed in response to legitimate concerns in the 1970s by the Foreign Intelligence Surveillance Act. "This is what we need for new technologies today. The black and white debate is not helpful," he said, "They are not opposing. We need to think about how to build one that supports the other. Here is the technology. How do we put something in place to make it safe to use [278]?" When asked to comment on MATRIX (Multi-State Anti-Terrorism Information Exchange), though, he added, "Matrix is not as dramatic or leading edge as TIA. However, we do have a similar problem in that police and law enforcement have a new set of tools and a new set of data. Suppose information gets in and it's wrong. How do you fix it? With any new technology we have to ask, "Do we have the right safeguards to protect privacy in place [279]?"

"I think some individual privacy will be lost," added Moseley, "I've spent the last thirty years with a security clearance. It doesn't bother me [280]." But Brad Martin spoke about privacy as a passive right. "You could lose it without even knowing it was gone," he said. Secretary Trent added, "Technology is probably the best thing and the worst thing that's happened to information security in terms of how the technology has allowed us to accumulate and digest more information than we have been able to in the history of mankind. At the same time, it exposes information that should be private [281]."

Calling the trade-off argument naïve, John Ripley said you needed to think about balancing trade-offs and offered another way to think about the issue, "What core liberties do you want to protect [282]?" Sophia Martinez agreed that, rather than think about the threat as coming from outside and hardening the target, she would rather consider concepts

related to security, such as privacy, the democratic process, and good international relations. "Computer security experts would have us start at the machine and move outward," she said, "I start at the outside and move in. I see the problem as a community or even international one [283]." Many of the panelists talked about heightened awareness since 9/11. "Everyone is more aware of and more conscious of security than three or four years back," said Jack Bailey. "The concept is evolving, added Arnold Madden. "Since 9/11, computer or network security has been thought of as more of a public safety issue, as we recognize the dangers of things like bio-terrorism or cyber-terrorism," he continued [284].

"The problem is not that you made a trade off," said Carroll Trask, "it is that average citizens have not had the chance to make the choice for themselves. This is what happens in times of crisis. Once the crisis is over and the cops and military make choices with the federal government, the citizen resents it and sees it as a trade-off. People feel like they are not involved. No one ever questions having a fireman or police. In terms of security, you have to get to the same place. It's a matter of choices you make. "For example," Trask added, "the local city hall may be deemed a critical asset in terms of public confidence. You can pile boulders up in front of the door. This is a choice you've made that security is more important than access. Was any freedom violated [285]?"

Matthew Barnes, though, indicated that, in addition to there being too little discussion of trade-offs between privacy and security, the other problem was that, while the focus is on security, the "so-called' security measures don't make us that secure. "I fly all the time and go through luggage searches and metal detectors. You can go to any gun

and knife store and buy a knife made of carbon fiber. I can tape that to my back and walk through a metal detector and get on a plane with a weapon." He added that the guiding principle should be the preservation of freedoms. "The flap now is that the government is trying to access all traveling records from airlines. Again, this is lazy thinking. If they were able to profile all airlines, terrorists would stop flying and come in through the Mexican border, which is wide open [286]." Several others joined in discussion of airport security procedures and intrusions to privacy, and being in a crisis mode. "In an airport, the ultimate security would be not to fly planes. Somewhere between that and letting everyone in, like we used to do, is the ideal," said Bob Moseley [287].

Mitchell Posner spoke about the need to learn about the priorities of citizens, "There's a question of how much people are aware about the intersection of technology and security or whatever you mean by those terms. People have things competing for their time. Maybe pollsters should find out. If you live in the DC area and are being told to buy duct tape and tape your windows shut, your perspective may be different. A gas bomb is technology. I suspect that people care about different pieces of security and technology in different ways. What people think about it doesn't mean it is right. This may help you to frame the issues and talk about this in ways that more genuinely reflect risks, consequences, and vulnerabilities. Having some sense of what people value and prioritize would help [288]." Carroll Trask explained that public confidence and morale are embedded in economic security, public safety, and national security [289]. "Privacy, the democratic process, and good international relations also have an affect on security," added

Sophia Martinez, “because they determine what is a threat in the first place. Where we are today has something to do with our history of threats and failures along the way [290].”

“Another interesting thing having to do with my piece of security; modern communications is full of people who manipulate fear,” said Karen March, “I resent this [291].” Ripley responded by explaining how the policy process, being reactive, emerges to deal with the external environment. “One problem with information security,” he said, “is that it got off to a bad start in that it was connected to the ‘dot.com’ boom and the accompanying exaggeration and misallocation of resources. Unlike in business, where you’d go out of business if you made a claim you couldn’t deliver on, it is difficult to disprove ridiculous claims in policy. “For example,” he added, “there could be a claim that hackers could shut down the entire electric grid for six months. How would you examine this? I say you have to look at what’s happening. There are lots of hackers out there, yet there is nothing to support a claim like this [292].”

There are real and exaggerated aspects to how this fits into the larger debate over national security policy,” he continued. “Most of the threats that are being talked about now were around during the cold war, but were put in a larger perspective. A bigger threat was the Soviet Union. Once that threat was removed,” Ripley added, “the other threats became inflated. After the cold war, the question became, ‘What are the new threats to national security?’ In response to that question, we hear about environmental security, health security, cyber security, and homeland security. In many cases, these threats involve improbable risk scenarios. It’s a little exaggerated, but this is what has shaped the debate. While proliferation-related weapons programs existed prior to 1992, they were

considered minor when compared with the Soviet Union. The Russians had twelve hundred ballistic missiles. The Koreans have one and we're not even sure if it works. You'd never know this from all of the noise, but this change in perspective has helped frame the security debate; the realization that we need to identify a source of risk." Shaking his head, Ripley added, "As soon as the cold war ended, I knew that all of these unemployed arms controllers would be looking for something to do [293]."

"Disclosure is the real issue," said March, "We're dealing with privacy, legal, and liability issues." Moseley added that there was talk of starting a new Internet that could only be accessed by Department of Defense and military computers, "I'm talking about security on the Internet. You'll have to give up freedom or you might have to give up using the Internet [294]." Alice Thompson, who had just returned from Abudabai and Dubai, spoke about the highly filtered Internet there. "It doesn't have many problems, but not everyone has freedoms [295]." Sophia Martinez joined in, "How does the culture of secrecy fit into a democratic context? Things must be done in a democratic fashion. If you take out the element of democratic dialog, you are not doing that and that becomes the model. It's terribly important that we keep this question in the forefront. Policy people need to keep asking that question [296]."

Secretary Dobrosky spoke of the bind this put him in. "As a citizen of the Commonwealth you could come and ask me for information on where our technology facilities are located and that might seem a perfectly legitimate question that you feel you have a right to have an answer to," he said. "But, if I gave you those locations, I would be exposing the state to some vulnerabilities. Where does my responsibility to keep this

secure conflict with your right to know [297]?" Dr. Posner spoke about his own background in private industry and how concerns of national defense and industrial espionage led to high levels of physical security and secrecy. "Being the sole supplier of nuclear fuel, when nuclear weapons were smuggled out of Kazakhstan," he said, "there were times when there were words that I could not say." Going on to explain that, at one time, he'd been given a list of certain geometric shapes that he was not permitted to say out loud, he added, "It was seen as a risk that people knowing where I worked and hearing me say the names of these shapes would put two and two together [298]."

Martinez ran into this culture of non-disclosure when, for educational purposes, she'd tried to obtain a diagram of her university's computer network. "It seems to exist, but nobody has one," she said, "I'm working to find an alternative theory having to do with hiding things in plain sight or recognizing the advantage of full disclosure [299]." The notion of hiding things in plain sight caused Matthew Barnes to speak up, "Have you heard of steganography?," he asked, "It has to do with hiding data in another artifact. An example would be digital technology where you take a picture or image, like a baby. It's a string of bits. In steganography, you can alter some of the bits to contain a code that delivers a message. If you viewed the picture, you couldn't tell if there was anything there. That's why giving the FBI more power to monitor networks does not guarantee that things will be more secure. There are very simple ways to avoid the monitoring [300]."

"Back to the question of what we are protecting," Dr. Thompson said, "if we are providing for a system of trust and the enormous possibilities for technology, how do you keep that going?" She added that there are two enemies of trust: bad character and bad

information and that it's possible for people to have good analytical processes, but poor emotional ones. "They can analyze a problem, but they don't know what to do with it [301]." Thompson reminded us that the original Internet was built on an architecture of trust. "People must be free to experiment, to create new ideas, processes, and products," she added, "If they become distrustful and insecure, they will not experiment unless their survival is threatened [302]" She went on to speak about the positive aspects of hacker culture. "There is a book, *The Cathedral and the Bazaar*," she said, "about hacker culture, hacker ethics, and hacker protocol." While Thompson recognized that there could also be a negative side, she emphasized the power of many minds working together [303]. On the other hand, a closed system also has negative aspects, she told us, and gave two definitions of a dead or dying system. "One is where boundaries are completely sealed off and it turns in on itself. The other is a system with no differentiation in its boundaries, so anything can come and go," she said. "If you lock a system down, is this what it will be for all time? Will it atrophy, turn in on itself, and die?" she wondered [304]. "As we move in this direction," Thompson continued, "the boundary between the last system and the next, the lawyers and psychiatrists are busy. These are the people who deal with the rules of the former system as we move into a new arena. This makes sense when you see how confused people are. Here we are in a context of very big security latching down like nothing that I have ever seen in my lifetime. Are we trying to latch down our biological systems, cultural systems, social systems, and information/ intellectual systems? Computing, information, and telecommunications technologies are the next infrastructure, but technology must remain hand in glove with content to benefit human learning [305].

Even though Lois could see the late afternoon sun shining through the window, the end of the program had seemed to arrive very quickly. It was interesting, she thought, that issues of disclosure and non-disclosure, open systems and closed systems, and whether there were trade-offs between security and individual freedoms had all been discussed in the technological realm, as well as the larger philosophical one. Beginning with looking at what we are securing, some focused on the technical securing of networks while others felt constrained by measures taken to enhance security and focused on cultural, moral, or ethical concerns, as being in need of securing. At the heart of concerns of technology and security, seemed to be the issue of access and restrictions to access and, in this latest discussion, we again ended considering the notion of balance, as opposed to trade-off, benefits of full disclosure, and the importance of an open environment for human learning. If Lois had learned anything, she thought, it was that you really had to pay attention to everything and that while that was probably impossible, a willingness to consider new information and new ideas was the only way you could possibly keep from excluding something that might be important. As she shook hands with conference participants and she made her way to her car, it dawned on Lois that what she saw in the rapidly changing world of information security characterized by ever increasing unforeseen threats really mirrored what seemed to be taking place in the physical world and that, while she witnessed efforts to consider information security in purely technological terms, it did not seem to be possible. Her own participation within the context of information security policy development had led Lois Lassiter to one conclusion. Everything matters.

Lessons Learned

If, indeed, we are to maintain a balance, as several had suggested, it may be important, as priorities seem to shift, to pay attention to the subjective, intersubjective, behavioral, and structural elements represented by the quadrants in figure 2 in the case study introduction. It is suggested that the reader keep this in mind as we discuss the following lessons learned and implications in the next chapter:

1. Security measures are not making us more secure.
2. The use of language and framing by policy advisors expands or limits the range of policy alternatives.
3. Policy makers rely on technological experts, among others, in developing information security policy.
4. There are problems with policy written in technologically specific language.
5. Sufficient policies are not in place to assure the quality of data being secured.
6. Information Security efforts since the September 11, 2001 may represent a conflict of interests.
7. There is disagreement about whether trade-offs between security and individual liberties are necessary.
8. There is disagreement about whether policies of non-disclosure make us more or less secure.
9. Information security policy has developed in a reactive mode.
10. There are ethical concerns about technological security measures.
11. It may be possible to expand the concept of “building in” security.

Chapter 5: Implications of the Inquiry

Lessons Learned

The previous chapter was written to provide an entrance into the world inhabited by the research participants in this inquiry. The purpose is for the reader of the research to become caught up in the context, to be exposed to a wide range of perspectives, and to gain understanding that will aid in policy development by expanding the range of issues and policy alternatives considered. The research question which guided my review of the literature, methodological choice, data collection process, emerging design, data analysis, development of the case study, and lessons learned is, "What is the meaning of security?" In this final chapter, I consider the meanings offered by participants in the research in terms of the lessons I've learned and the implications of those lessons. Before I do so, however, it seems important to mention that these lessons do not represent all that is possible to be gained from the research. Rather, they demonstrate my specific interpretation, based on my subjective understanding of the interaction that took place and what resonated most with me. It is my hope that in providing a rich characterization of the research context, I have left the door open to others with related interests to also become a part of the research experience by juxtaposing their perspectives with others and determining the meaning of this inquiry for themselves in their own settings.

As I noted in chapter four, data have been organized in terms of four major categories. These are: *What are you trying to do?*, which consists of all data relating to mission and desired outcome; *Security and Technology Issues*, which includes data regarding access, security programs, technology, legislation, implementation problems, and risk assessment; *Language and Framing*, which includes all data relating to language and the way information is presented; and *Balance and Trade-Offs*, which includes data relating to issues of individual freedom in relation to public safety. These are then further divided into a number of sub-categories.

What are you trying to do? relates to *Security and Technology Issues*, as security measures taken will depend upon what it is seen as in need of securing. For example, if the goal is protecting data, technological measures will be different than if the goal is protecting users. These goals are determined by processes of risk assessment, which allow risks or threats to be viewed in particular ways, thus eliciting a certain kind of technological response. As assessments of what constitutes a threat appear to depend, in large part, on who is involved in conversations about risk, definitions used, and the way information is presented to those who make decisions, *Language and Framing* become an element in all of the categories, including *Balance and Trade-Offs*; as emphasis on public safety or civil liberties cast issues in a particular light or whether threats, such as terrorism, are seen to be external, requiring pre-emptive anti-terrorism solutions, or rooted in internal factors that may have contributed to our being at risk. The hermeneutic process is evident both in the linking of the categories and in the circular nature of the presentation of the data.

In addition, the nature and complexity of participant responses led to the development of four Meta-categories: *subjective* responses, in which participants offered their opinions; *intersubjective*, in which they spoke in moral and cultural terms; *behavioral*, in which they spoke of concrete action taken to resolve specific problems; and *structural*, in which their responses reflected legal or procedural measures. As a preface to my lessons learned, I'd like to suggest that participant responses might also be considered in terms of: what is not working, why it is not working, what we might do differently, and how that might be accomplished, noting the values that underlie those suggestions.

It has been suggested that without a systemic understanding of the world, change may be impossible (Collins, 1997; Harstock, 1987). If knowledge depends on experience, then the ability to experience a variety of perspectives may enhance the quality of knowledge necessary to make change possible (Hundleby, 1997). While analyses of standpoint may differ by discipline (Harding, 1997) and the value of a particular perspective may weigh in differently, it may be through the openness to the totality of perspectives and the ability to experience the worlds of others (Smith, 1997) that will truly allow change to take place. Recognizing that there are a number of ways to make sense of the context, I'll also suggest that with each interpretation, we learn more. I begin by offering this one.

Lesson 1: *Security measures are not making us more secure*. While federal and state governments and universities conduct risk assessments, develop standards, and engage in partnerships with private industry to research technological security solutions, participants from all groups noted that attempts to make us more secure are not working.

There were a number of reasons given for this. Some participants pointed out that cost/value considerations and rigid standards do not work in a university environment where costs translate into reductions in service. Others noted that data cannot be guaranteed one hundred percent and that measures to do so will inevitably fall short. While it was acknowledged that the assumption of a threat is built into risk assessment, there was a consensus that the threats are constantly changing, that we do not know what they are, and that the challenge is in preventing something from happening that hasn't yet occurred. Along with this, came concern that there is an emphasis on searching for new threats and that there is really no way to determine if these threats are real or exaggerated. It was also suggested that public safety measures, such as those instituted by the Department of Homeland Security, increasing the power of law enforcement officials, are based on the notion that experts know better than the average citizen and that there is no evidence of this. In fact, many of the participants in this research are considered to be experts and the consensus was that experts are extemporizing.

This research and the literature both suggest that, in light of the complex nature of information security policy development, more research is needed in alternatives for traditional risk assessment (National Commission, 2004; Sarewitz, Pielke & Keykhah, 2003). Although the data indicate that there is agreement that the notion of a threat is built into risk assessment, it is not clear exactly what constitutes a threat. This research suggests that there are ways of assessing risk other than "hardening the target" and recognizes that supporting the adoption of a community or international perspective, with an emphasis on sharing, could both reduce risk and improve understanding of factors leading to the U.S.

becoming a target. This has implications for policy makers who may be able improve security by re-framing issues as global concerns that call for shared efforts. There are also implications for researchers who may be interested in exploring the meaning of risk.

Lesson 2: *The use of language and framing by policy advisors expands or limits the range of policy alternatives*. This research indicates that the words that are used and the manner in which issues are presented to policy makers result in their perceiving issues differently and recognizing a different range of alternatives. The data also suggest that the way an issue is framed can determine who is present in policy discussions. Examples included information security issues framed as information technology issues and turned over to IT departments, HIPAA's being framed as a health issue as opposed to a security issue or a privacy issue, and the predominance of law enforcement agencies in the formation of the Department of Homeland Security. The data suggest that by defining its mission in terms of public safety, DHS was able to proceed with electronic surveillance and other security measures without public debate by calling on the public to trust the experts in a time of emergency and presenting a scenario in which only two alternatives were offered, civil liberties or public safety. Participants spoke about the need to choose framers and words carefully, the importance of clear explanations, and recognized the use of metaphor, such as master cylinders and controls, in influencing the way we consider issues. This has implications for policy makers for whom issues are framed and presented prior to policy development and seems to require that attention be paid to how issues are presented, who is presenting them, and who is being left out of the discussion. In addition, attention to language and the images conjured up in response to information presented may

allow policy makers to see how those images can be transformed by altering the words used to describe them and, by doing so, inform policy. There are also implications for research into language development and use in unstable or rapidly changing environments.

Lesson 3: *Policy makers rely on technological experts, among others, in developing information security policy.* This study indicates that there is concern about those to whom policy makers look for advice, as well as their reliance on a small circle of advisors representing too narrow a perspective. The data show that, for some policy makers, information security policy development begins with those who understand the technical workings of networks and systems and then is reacted to by others. Working hypotheses that both terminology and values for these groups differ seem to be supported by the research. However, there is also evidence that definitions for each group are not static, but change to suit the specific context or audience. Likewise, in all settings, policy makers and technologists support a number of values that, at times, can be seen as being in conflict with one another, as they respond to demands for open and restricted access to information. If, as the literature suggests, policy makers are often not involved, in policy definition (Kanner, 2001), there are implications for policy makers, as their own values and perspectives may not be given full consideration in the advice they are offered and from which they make policy decisions. Research implications include the need for the development of models or frameworks that assure the inclusion of diverse points of view in the policy process.

Lesson 4: *There are problems with policy written in technologically specific language*. This research reveals a number of problems with policies that are written in

technologically specific language. Concerns range from such practical considerations as policies becoming outdated too quickly, as the technology changes, to concerns that technological language could result in narrow interpretations that would make policies irrelevant in certain situations. Participants used encryption and copyright as examples of areas where problematic laws have been written in technologically specific language and also pointed out that liability issues could result from policies requiring specific technology, as compliance would require adhering exactly. The data indicate that, depending on whether an issue is framed as an information technology issue or an information security issue, the language will be different. This research further suggests that an effective strategy for developing policy involves focusing on *what* it is that a policy is to accomplish instead *how* it will actually be accomplished.

There is evidence that policy written too narrowly in technologically specific language has resulted from both placing responsibility for information security policy writing in IT departments and from policy makers relying on the advice based on the interests of lobbyists for a particular industry. Implications for policy makers include recognizing the importance of a wider range of perspectives in developing information security policy and realizing the limitations of technological advice. Unless policies are being written for technical staff to carry out very specific procedures, this research suggests that responsibility for policy development should not lie with IT staff, but with policy makers who are prepared to consider issues from a broad perspective. If, as these data suggest, there is a need to develop a language or languages to promote clarity and assure even-handedness as policies are developed, there are implications for research in

exploring policy language both in terms of encompassing complexity and in its ability to allow policy to remain accessible to citizens.

Lesson 5: *Sufficient policies are not in place to assure the quality of data being secured*. Participants in this research acknowledged that it is difficult to discern good information from bad, that security is only relevant if it protects something you value, and that information is only valuable if it is used. As government and industry engage in information sharing of data about individuals, criteria need to be developed not only to determine the kinds of data to be collected, but also for assuring its quality. The literature indicates that oversight does not exist for maintaining accuracy in consumer databases, that it has been left largely to the consumer to monitor (Nehf, 2003), and that there are significant problems maintaining accurate databases on non-citizens (Schulman, 2002). If this is the case, individuals do not only have the privacy of their information to be concerned about, but also its accuracy. This also raises concerns about the effectiveness of information sharing when information is incorrect and has implications for policy makers in that policies and procedures for assuring the quality of information being secured must be in place before other policies regarding its use are developed and implemented. However, this research also has implications for research, suggesting that future scholarship should not be limited to a focus on the development of procedures in the present environment, but ought also to address alternatives to information sharing and government oversight raised by this inquiry.

Lesson 6: *Information security efforts since the September 11, 2001 may represent a conflict of interests.* An increase in security programs, the development of university

security institutes, and partnerships involving universities, government, and the private sector for research and development of devices to fight cyber-terrorism and protect the critical infrastructure have all occurred in response to the 9/11 terrorist attacks. This study indicates that there is concern over a lack of discussion about trade-offs between public safety and civil liberties. The data suggest that more public discussion needs to take place with regard to due process, treatment of immigrants, and how we determine how liberties will be extended to non-citizens. Another concern reflected in the data is that, as partnerships are formed among universities, government, and the private sector, the neutral position of the university could be compromised. This study indicates that universities are actively engaged in research involving anti-terrorism and critical infrastructure protection and seek federal grants to further develop surveillance and other information security measures. The data suggest that there is concern that policies of non-disclosure and restrictions about dissemination of research results are counter to tenets of academic freedom. This research further indicates that greater restrictions, controls, and secrecy are being called for by the private sector, which owns most computer networks and have a financial stake in critical infrastructure protection. If this research represents an accurate portrayal of the context, there are implications for policy makers. There appears to be evidence that values of all stakeholders may not all be given credence as partnerships are formed between and among them, which supports what was found in the international literature (Barbosa, 2003; Byrne & Weir, 2004; Diken & Lausten, 2004; Foster, 2003; Kelly, 2003; Sayegh, 2004). If these partnerships are to continue, efforts must be made to assure that private or law enforcement interests do not result in agenda setting or policy

development that favor economic interests over individual liberties or humanitarian concerns and discount the importance of public debate. With regard to research, the data suggest the need for research into what is important to individual citizens with regard to the interplay of security, technology, and privacy.

Lesson 7: *There is disagreement about whether trade-offs between security and individual liberties are necessary.* There are conflicting data on whether trade-offs between security and individual liberties are necessary. In addition to responses supporting the notion that trade-offs between security and individual liberties are inevitable, there are also data supporting the position that it is possible to protect core liberties and balance security with individual liberties. Data include concerns about security at the expense of privacy, functional privacy that's been lost through technological changes, surveillance measures outlined in the *USA Patriot Act*, and loss of due process. This research suggests that both security and individual liberties are important values and that one need not be sacrificed for the other. The data include responses indicating that a balance needs to take place and suggest considering questions such as what core values we want to keep or what kind of community we want. While the data also include statements to the effect that trade offs are necessary, this was not the consensus. If this research is accurate, it is possible that rhetoric outlining a trade-off between security and individual liberties has been an attempt to over-simplify a complex issue. This has implications for policy makers. As efforts to simplify complex problems are tried and fail to work, policy makers may need to look for other ways to develop policy in a complex environment.

Based on the data and the literature, there also appear to be implications for research, as theories, frameworks, and strategies related to complexity and decision making are needed.

Lesson 8: *There is disagreement about whether policies of non-disclosure make us more or less secure*. Efforts to secure information include the exemption of security related information from *Freedom of Information Act* related requests and the institution of a policy for release of information based on a "need to know" (Ashcroft, 2001; Feinberg, 2002). This research indicates that there is concern about attempts to maintain a culture of secrecy within a democratic context. The data further suggest that a policy of full disclosure, which allows for failures to be revealed, may actually do more to promote a secure environment. Legal measures taken to prevent publication of research revealing flaws in existing encryption codes were cited as an example of how secrecy could prevent further research needed to secure information.

Some considered the open environment of the university to be a security problem. Others saw it as more secure than the commercial world in that it fosters an environment in which new information and ideas are freely considered, failures revealed and learned from, and anxiety that works as a barrier to change is lowered. The data also suggest that, if information technologies are to become the next infrastructure, technological developments must complement human learning. If, as the data suggest, innovation occurs in an environment of trust where people are free to experiment, policies inhibiting the exchange of information may result in a closed or dying system. If policy makers are to develop effective policies that incorporate democratic ideals along with security measures, they must take into account the benefits of open systems that allow for diverse input as

well as closed systems that limit access. Scholarship in this area might benefit from a mapping of the information security terrain that allows for new meanings of security to be considered alongside physical security definitions, which, so far, have provided the basis for thinking about security of data.

Lesson 9: *Information security policy has developed in reactive mode*. This research indicates that information security policy is developed in response to threats, many of which are unknown. In addition, the data suggest that a search for new sources of risk has shaped the information security policy debate and has led to exaggerated claims which cannot be examined. This study suggests that this strategy may have contributed to a mindset in which threats are classified as external, resulting in policy responses that are reactive. Participant responses included both a recognition that everything is vulnerable and concern that the fear engendered, by focusing on this vulnerability, has been manipulated to set public policy without public debate. The data suggest that adopting a larger frame of reference incorporating democratic values and international perspectives would provide insight into the current environment. The data further suggest that thinking in global terms about what kind of community we want and sharing responsibility would contribute to better understanding about the nature of threats. Implications for policy makers involve the willingness to listen to advice that this study categorizes as subjective and intersubjective, as well as the behavioral and structural perspectives that seem to drive the current thinking about information security policy. The data indicate that policy makers need to look for patterns to help them discuss the big picture. This study has implications for researchers in public policy and administration who are interested in

exploring ways to assure the incorporation of multiple perspectives in policy and decision making.

Lesson 10: *There are ethical concerns about technological security measures*. Participants in this study both marveled at what could be done with technology and had concerns that the fast rate of technological development was causing questions to be raised for which we do not have ethical answers. Although it was suggested that technology enhances individual privacy by eliminating the human factor in security, the data strongly confirm that most of the participants had some degree of concern about invasions of privacy due to advances in technology. The data include a wide range of troublesome issues including, surveillance in public places, monitoring of computer use in universities, and large scale information sharing by linking databases. This research reflects concerns that privacy can be lost without the average person knowing it's gone and suggests that citizens know very little about how technological approaches to security can invade their privacy. Technological security measures were also seen as threats to academic freedom in their monitoring of student computer use and in attempts to limit access to ideas, as well as networks.

Although data include statements to the effect that security must always be seen through the prism of individual rights and that policies need to go through a civil liberties filter, concern exists that this is not being done. While some attributed this to an increased focus on security since 9/11, there is evidence that the speed of technological development and the framing of the security debate as one in which we may have to temporarily give up liberties to have security have both contributed to a policy of proceeding with

technological security measures without fully attending to their ethical implications or possible ramifications for society.

This study indicates that the way in which an issue is framed can result in the inclusion or exclusion of certain political actors. By framing information security narrowly, as primarily a law enforcement issue or a technology issue, other important societal values may be left out of the policy development process. Based on this research, implications for policy makers include an obligation to make sure that citizens are informed, to proceed with any security measures based on democratic values, and to include the broadest possible range of perspectives in considering policy alternatives. Research in this area might focus on the development of a framework to be used for making ethical decisions within a context characterized by complexity and competing values.

Lesson 11: *It may be possible to expand the concept of "building in" security*. This research indicates that the concept of "building in" security is being considered by technologists as an alternative to developing patches to respond to cyber threats. Building in security relies on shifting the focus away from responding to external threats and onto strengthening existing mechanisms. Participants indicated that building in security from the beginning is a good security principle and recognized that the same processes that work to prevent malfunctioning can also work to deter external threats.

In addition to shifting from a reactive stance to one that focuses on building on strengths, this research suggests that this is an approach that requires systematic thinking, an ability to visualize what a product will look like when it's done, and the insight to

recognize what it will take to get there. The data further suggest that the lack of a holistic view and policy makers' asking the wrong questions have resulted in problematic information security policy with unanticipated consequences. Although the data include references to holistic thinking and systems analysis with regard to building in security, there is no evidence that these terms were used to incorporate perspectives outside of the technological arena. However, this may be an appropriate area for further exploration if, as the literature suggests, vulnerability can be viewed as a human rights issue (Sarewitz, Pielke & Keykhah, 2003). If this inquiry offers an accurate reflection of current reality, it may be that a systems approach expanded to include intersubjective data would allow some of the concepts used in technology to be used in policy making. For example, there may be parallels between questions like, "What kind of community do you want?" and "What will it look like when it's finished?" The data in this study suggest that building in security on a technical level requires starting with the end in mind and visualizing the steps it will take to get there. This has implications for policy makers, as it could require a greater willingness to be attentive to a wider range of perspectives and a wider range of data for consideration. There are also implications for researchers interested in a macro approach to security theory that incorporates community or international perspectives.

Implications of the Inquiry

As the quality of the constructivist inquiry can perhaps best be gauged by its usefulness, I'd like to further discuss implications of this case study and my lessons learned. In order to both provide a sense of balance and to demonstrate how this research fits with what has come before, I will organize my remarks and discuss implications that I

see for policy makers and for research within a framework offered by the existing literature. As I do my best to fill in missing pieces in the security puzzle, I realize that other gaps may be exposed, as new meanings offered also raise new questions. Through this attempt to parallel the hermeneutic process, it is my hope that an understanding, incorporating the multiple meanings of security presented here, will emerge and be useful to readers.

The Limitations of Language

Before security measures can make us secure, we must possess an understanding of what it means to be secure and assess whether or not that can be achieved. The context described in this research is clearly one in which security has many meanings. Sometimes language allows us to consider shades of difference, for example, one participant mentioned the many words used to describe different kinds of snow. At other times, language is limiting in that the terms we use to describe a phenomenon can't quite capture the essence of what we are trying to say. However, it is not enough to realize these limitations if we then proceed using language that forces us to leave out important considerations. It is my contention, based on my understanding of the research context, that efforts to cast information security questions in a technological, economic, or public safety light have been attempts to simplify them.

Much has been said in this report about the role of technology both in talking about information security and in policy development. By taking a technological approach, actors in this arena are trying to break down a complex problem into smaller pieces, each of which seems comprehensible. The trouble is that the sum of the smaller parts does not

appear to equal a whole that represents current reality. A positivistic approach is helpful when we can isolate variables and zero in on some aspect of reality to prove a truth that can later be applied in other contexts. It is, perhaps, the mathematical underpinnings of technology, which allow for reductionistic problem solving, that make it attractive to those who are looking for absolute answers and seek to discuss concepts in concrete terms. However, it seems clear that the questions we face in this inquiry are not simple and definitions are not constant.

If using the language of technology is one way to cast security in a scientific light, applying the language of business appears to be another. Attempts to assess risk in the environment studied use cost/value formulas and arise from an orientation where profitability underlies action and money spent on security is viewed as the cost of doing business. Both technological and business approaches to information security appear to be attempts to simplify a complex problem by considering it in exclusively scientific or economic terms. A third attempt to simplify information security questions can be seen as issues are described in terms of public safety and law enforcement. Adopting a definition of security from law enforcement allows for a security to be described as something that can be enforced and for factors standing in the way of enforcement to be counter to security, resulting in what some participants referred to as a "black and white" debate (Huysmans, 2002; Menjivar & Kil, 2002). While each of these frameworks for considering issues of information security taken individually, obviously leaves out part of the picture, we may still be limited if we consider them together. Here we have science, economics, and the law, but what is missing and what are the implications?

Not only does it appear to not be helpful to break down the complex issues surrounding information security in developing effective security measures, if the data and the literature are to be believed, attention to complexity is essential (National Commission, 2004; Pauchant & Mitroff, 2002; Ostfield, 2004; Raab & Milward, 2003; Wise, 2002; Zahariadis, 2003). What's more understanding of the environment is being said to call for recognition of interconnectedness, not only among disciplines, but among data representing individual and collective values, as well as strategies and formal standards or procedures (Wilber, 2000). The context depicted in this research is one in which information security policy development is being hampered by policy makers attending to advice from too few advisors who are framing issues and using language in ways that exclude others from the discussion. Several in this study spoke about the need to enlarge the frame or consider the big picture. Interestingly, even when participants spoke about taking a systems approach or seeing the bigger picture, they still held limited views in that they were rarely aware of what it was that they did not know or what perspectives were missing. The literature supports the notion that *intermediaries*, *integrators*, or *change wizards*, who can not only see the big picture, but remain attentive to an ever expanding picture, are needed (Beck & Cowan, 1996; Rein, 1974; Wilber, 2000). If efforts to simplify complex problems by breaking them down do not work, then policy makers must find other ways to resolve problems and develop policy within a complex environment.

Implications for policy makers include the need to seek advice from advisors representing the broadest possible range of perspectives and a willingness to temporarily adopt these perspectives in order to inform policy decisions and anticipate possible

unintended consequences (Balfour & Mesaros, 1994, Farmer, 1998). In addition, attention to nuance and the use of language to persuade could help policy makers to more easily recognize attempts to influence them. With regard to the meaning of security, the word security seems inadequate for incorporating the multiple meanings revealed in this research. While this study includes data indicating that some working in information security seek to form a common language, those efforts rely on incorporation of words and languages that already exist. It would be more advantageous to, as the literature suggests, develop languages that include all we wish to say (Day, 2001). Future research needs to focus on development of models that, rather than respond to change, allow for complexity so that new words and new perspectives can continually be added to the mix without discarding others. While Wilber's (2000) integral theory helped to provide a way for me to conceptualize what my data analysis was revealing, it also offers just such a framework and may have application for public policy and administration.

Technology, Security, and Society

This research supports the assertion in the literature that there are multiple meanings for the words *technology* and *security* (Dhillon & Backhouse, 2001; Ellul, 1964; Illich, 1973; McOmber, 1999; Spight, 2000; Weber, 1958). In spite of awareness on the part of most of the participants that diverse definitions exist, policy development appears to be based exclusively on the assumptions of those advising policy makers. For many, these assumptions come out of IT departments and reflect a technological approach to security. However, the situation is really much more complex when we consider the

interests of private industry in protecting the critical infrastructure and the government's interest in partnering with private industry and universities for research in anti-terrorism.

One aspect of this complexity depicted in this context can be explained in terms of values. The university values the open exchange of ideas and academic researchers seek funding the furtherance of knowledge. Private industry values research in that it is necessary to protect their financial interests in the critical infrastructure and to help them stay one step ahead of the competition in developing cyber solutions, but does not support the openness valued by academia. The government's position is one that strives for the public good, which includes an educated society, and seeks to defend society from terrorism by partnering with the university and private industry. This research raised questions about the clash of these differing cultures and the data suggest that there are concerns about possible ramifications of partnerships between government and industry on the university and academic freedom and on the public's right to know. The data also suggest that, while universities have established security institutes and demonstrate concern over government standards and control, there is no evidence that the influence of private industry on government has been addressed.

This research suggests that policies written in technologically specific language are problematic and that one of the reasons policy has been developed this way has been in response to profitability concerns of the publishing and motion picture industries who have sought to extend copyright protections. The data indicate that this has also resulted in concerns about academic freedom with regard to fair use, the dissemination of digital copies, and the ownership of created works and knowledge. This study reveals that, along

with business interests, the pace of technological development has also influenced information security policy development. This is evident in concerns participants expressed about privacy and electronic surveillance measures permitted by the *USA Patriot Act*. However, there is also data to show that concerns about privacy have occurred in response to government efforts to share information on individuals by creating large databases from a variety of sources.

If this research has accurately captured the interplay of technology, security, and society, it is clear that they are inextricably linked in a number of ways. The implication for policy makers here is that it seems clear that these elements cannot be considered in isolation. To do so is to engage in what Lyotard (1984) referred to as a game in which one uses discourse to simply legitimate a point of view. In our case study, Lois Lassiter ended by saying that everything matters. However, it might be more accurate to say that everything matters in different ways, to different degrees, at different times. Further, we cannot say with certainty what perspective might offer a solution at a given moment (Rorty, 2002). If, as in this context, the future is full of unknowns, an approach that allows for flexibility and inclusion of new information is superior to one that relies on only past experience or the need to predict the future.

Data Protection

While technological innovation has contributed to situations that have given rise to new ethical dilemmas, such as whether or not the government should compile large databases to share information on individuals or monitor their activity, there are related concerns about the quality and accuracy of that information. Data have been collected by

different agencies, organizations, or businesses, for a variety of reasons, with different standards for updating and maintaining accurate records (Schulman, 2002). Although it is possible that the lives of U.S. citizens could be adversely affected by relying on incorrect information in MATRIX or due process denied to foreign students registered in SEVIS, measures to safeguard the accuracy of information already in databases discussed by participants were limited to data entry. In addition to concerns that efforts may be going into protecting incorrect information, participants spoke about indiscriminate collection of individual citizen data and raised questions about just how much information the government needs and for what purposes. It was also suggested that information sharing has become an endgame, resulting in a focus on the process rather than a deliverable. This research indicates that implications for policy makers involve facing moral and ethical questions about whether information on individuals should be shared and, if so, how much and what kinds of information. In addition, if information sharing is to take place, the issue of accuracy of data needs to be addressed, as well.

"Building in" Security

The attacks of September 11, 2001 have resulted in a number of security measures including some which raised concerns for participants in this study about too little public discussion about trade offs between security and civil liberties and whether they are necessary, that public policy reflects a reactive or defensive stance, and that fear of the unknown is being used to manipulate the public. The writings of Richard Rorty and Martin Rein, that have served as a framework for conducting this research, may be useful in considering its purpose here. While Rein (1976) recognizes the necessity of framing for

making problematic situations comprehensible, Rorty (1999; 2002) emphasizes the importance of freedom and openness in reaching consensus on workable solutions.

The data suggest that a re-framing of the security debate as one in which it can be considered as a global or community problem with shared responsibility might allow policy to be developed with more consideration of shared values and less of an emergency stance. It was interesting that discussion of sharing and looking for patterns to view the big picture seemed to lead back to the benefits of full disclosure, as opposed to non-disclosure, that had arisen in the university's contention that an open environment made them more secure than the secrecy of the business world. If, as this research indicates, the issue of open v. closed environment has implications for teaching and learning and that the free exchange of ideas, looking at things in new ways, admitting failures, and recognizing that good ideas can come from unexpected places, there are also implications for information security policy, for relationships among universities, governments, private and non-profit organizations, and human beings. In the discussion of electronic surveillance and monitoring, one participant mentioned steganography, which allows data to be hidden in another artifact, and makes electronic monitoring ineffective. This same notion of hiding information in plain sight was also introduced for broader consideration as another participant spoke of the need for finding a theory of security that recognizes the advantages of full disclosure. This has implications for research in the development of theories that attend to complexity through openness and full disclosure. Implications for policy makers include the need to recognize the complexity that exists and be open to focusing on the flexibility that will let them find ways to adapt to, rather than react to, the environment. It

is unlikely that changes like this will be either easy or comfortable. Adopting such an approach to policy making would require facing the paradox that greater security may grow out of a recognition that complete security cannot exist. It would require movement from a mandate of certainty to one of openness to potentiality and an admission that current security measures are not working. However, what may be more effective than criticizing existing practice, is the suggestion of an alternative.

What is suggested here is an alternative that allows for the imagination necessary to envision a scenario of political action capable of taking us from the present into the future (Rorty, 1993). This view would not necessarily require policy makers to change actions taken or policies developed; what it would require is for them to change the way they think about what they do. In this process, they would be open to the emergence of new ideas and new ways of doing things (Rorty, 2002). Along with this would need to come recognition of multiple perspectives and a valuing of the wide spectrum from which new ideas could emerge. In the current socio-political context, it may be difficult for some to embrace the benefits of imagination and intersubjective agreement. If, however, as the research suggests, current methods for developing information security policy are inadequate in a complex world; it may difficult to argue against being open to new vision or the utility of a policy for which consensus has been reached (Rorty, 2002; 2004).

As I close this chapter, I am both excited by all that I have learned and overwhelmed by a realization that my experience has just scratched the surface of a myriad of new information and new ways of seeing things. It is reassuring to me to acknowledge that one cannot really seek answers to big questions and expect them to be good for all

time in all places. In a complex world in which policy and action can quickly become outdated, what would be valuable is an approach that allows for and gains from that complexity. Taken together, the advantages of full disclosure, the inclusion of multiple perspectives, the recognition that good ideas can come from unexpected places, the importance of inter-connectedness, and the ability to look at things in new ways may allow us to begin with the concept of "building in" security, presented here in technological terms and expand that concept to allow for disparate and complex data to be considered as we work to "build in", for lack of a better word, *security*.

References

References

Adams, J. (2001). Virtual Defense. *Foreign Affairs, 80*. 98-112.

Advisory Panel Reports on Cyber Terrorism. (2000, December 14). *Tech Law Journal*. Retrieved July 22, 2002 from http://www.techlawjournal.com/alert/200012/20001214.asp.

Albarran, A.B. & Goff, D.H. (2000). *Understanding the Web: Social, Political, and Economic Dimensions of the Internet*. Ames, IA: Iowa University Press.

Altbach, P.G. (2001). Academic Freedom: International Realities and Challenges. *Higher Education, 41*. 205-219.

American Association of University Professors. (2003, November/December). Academic Freedom and National Security in a Time of Crisis. *Academe*. 34-59.

Anderson, L. (2003). *Pursuing Truth, Exercising Power: Social Science and Public Policy in the Twenty-first Century*. New York, NY: Columbia University Press.

Ash, T.G. (2003). The Banality of the Good. *New Statesman, 16*. 12-13.

Ash, T.G. (2004). Living with America: It's Four More Years. Here's How the World Can Turn Them into Opportunity—in Partnership with America. *Newsweek International*. Retrieved November 29, 2004, from InfoTrac OneFile database.

Ashcroft, J. (2001, October 12). Memorandum for Heads of all Federal Departments and Agencies: The Freedom of Information Act. Memo posted to http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm.

Baker, J.C. & Williamson, R.A. (2000). The Implications of Emerging Satellite Information Technologies for Global Transparency and International Security. In B.I. Finel & K.M. Lord (Eds.), *Power and Conflict in the Age of Transparency* (pp. 221-255). New York, NY: Palgrave.

Baker, N.V. (2002). The Law: The Impact of Antiterrorism Policies on Separation of Powers: assessing John Ashcroft's Role. *Presidential Studies Quarterly, 32*. 765-779. Retrieved July 2, 2004 from InfoTrac OneFile database.

Baker, N.V. (2003). National Security versus Civil Liberties. *Presidential Studies Quarterly, 33*. 547-568. Retrieved July 2, 2004 from InfoTrac OneFile database.

Balfour, D.L. (1994). Connecting the Local Narratives: Public Administration as Hermeneutic Science. *Public Administration Review, 54*. 559-564.

Balkin, J.M. (2004). Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society. *New York University Law Review, 79*. 1-58.

Barbosa, R.A. (2003). Post-9/11: A Brazilian View. *World Policy Journal, 20*. pp. 75-81.

Beck, D.E. & Cowan, C.C. (1996). *Spiral Dynamics: Mastering Values, Leadership, and Change*. Malden, MA: Blackwell Publishing Ltd.

Behrens, T.R. (2001). Unintended Consequences of Cooperative research: Impact of Industry Sponsorship on Climate for Academic Freedom and Other Graduate Student Outcome. *Research Policy, 30*. 179-199.

Berman, J. & Bruening, P. (2001). Is Privacy Still Possible in the Twenty-first Century? *Social Research, 68*. 306-318.

The Big Picture: The Federal Government's Geospatial One-Stop Portal Holds the Promise of Better Homeland Security. (2003, September). *Homeland Security: Finding Common Ground (A Supplement to Government Technology*. 10-12.

Bogdan, R.C. & Biklen, S.K. *Qualitative Research for Education: An Introduction to Theory and Methods*. Boston, MA: Allyn and Bacon.

Bonner, R.C. (2003, September 12). Securing America's Borders While Safeguarding Commerce. *Heritage Lectures*. 1-7.

Borrego, A.M. (2003). Homeland Security Bill Would Provide $125-Million for a Group That Includes 3 Universities. *The Chronicle of Higher Education*. Retrieved June 18, 2003 from http://chronicle.com/daily/2003/06/2003061801n.htm.

Bouma, G.D. & Atkinson, G.B.J. (1995). *A Handbook of Social Science Research, 2nd Ed.*, New York, NY: Oxford University Press.

Braman, S. & Roberts, S. (2003). *New Media & Society, 5*. 422-448.

Buber, M. (1958). *I and Thou*. New York, NY: Scribner.

Burrell, G. & Morgan, G. (1979). *Sociogical Paradigms and Organizational Analysis*. London, UK: Heineman.

Bush, G.W. (2001). *Executive Order: Critical Infrastructure Protection in the Information Age*. Office of the Press Secretary.

Byrne, I. & Weir, S. (2004). Democratic Audit: Executive Democracy in War and Peace. *Parliamentary Affairs, 57*. 453-468.

Carey, D.W. (2003, May). *Information Assurance Post 9-11: Enabling Homeland Security*. Oracle Corporation.

Carlson, S. & Foster, A.L. (2002). Colleges Fear Anti-Terrorism Law Could Turn Them Into Big Brother. *The Chronicle of Higher Education, 48*, A31.

Carnevale, D. (2001). Network Practices Can Endanger Students' Privacy, Report Warns. Chronicle of Higher Education, 48. 1-2. Retrieved November 21, 2002 from http://chronicle.com/weekly/v48/i13/13a03002.htm.

Carnevale, D. (2002). Logging in with Bradford C. Brown: George Mason U. Center Studies Legal Trends Related to Network Security. *The Chronicle of Higher Education, 48*, A36.

Carrageen, K.M. & Reefs, W. (2004, June). The Neglect of Power in Recent Framing Research. *Journal of Communication*. 214-232.

Carroll, J.S. & Johnson, E.J. (1990). *Decision Research: A Field Guide*. Newbury Park, CA: SAGE Publications.

Cello, J. (2002). This Perfect Day: The Road to Hell is Paved with Good Intentions. *Intelligent Enterprise, 5*. 64-65. Retrieved October 5, 2004 from InfoTrac OneFile database.

Chomsky, N. (2001). *9-11*. New York, NY: Seven Stories Press.

Chomsky, N. (2001a). *Propaganda and the Public Mind: Conversations with Noam Chomsky*. Cambridge, MA: South End Press.

Chomsky, N. (2001b). The United States is a Leading Terrorist State. *Monthly Review, 53*. Retrieved November 22, 2004, from, Expanded Academic ASAP database.

Chomsky, N. (2002, September/October). The Crimes of 'Intcom.' Foreign Policy. pp. 34-35.

Chomsky, N. (2002a). A World Without War? Reflections on Globalization and Antiglobalization. *Canadian Journal of Development Studies, 23*. 493-511.

Chomsky, N. (2003). Commentary: Moral truisms, empirical evidence, and foreign policy. *Review of International Studies, 29*. 605-620.

Chomsky, N. (2003a). One man's world: George Bush's men have made the grand strategy explicit. But the belief that the US is above international law began long before this president. *New Statesman, 132*. Retrieved November 22, 2004, from Expanded Academic ASAP database.

Chomsky, N. (2003b). *Power and Terror: Post-9/11 Talks and Interviews*. New York, NY: Seven Stories Press.

Chomsky, N. (2004, March 14). How America determines friends and foes. *The Toronto Star*. Retrieved November 23, 2004, from Factiva database.

CISC. (July 2001-June 2002). Annual Report – Year One: Advancing Virginia's Information Security Expertise.

Collins, P.H. (1997). Comment on Hekman's "Truth and Method: Feminist Standpoint Theory Revisited": Where's the Power? *Signs, 22*. Retrieved December 1, 2004, from Expanded Academic ASAP database.

Cowan, C.C. & Todorovic, N. (2000). Spiral Dynamics: The Layers of Human Values in Strategy. *Strategy & Leadership, 28*. 4-11.

Creswell, J.W. (1994). *Research Design: Qualitative & Quantitative Approaches*. Thousand Oaks, CA: SAGE Publications.

Dawson, S., De Capitan did Venerate, S., Lincoln, P. & Samurai, P. (2002). Maximizing Sharing of Protected Information. *Journal of Computer and System Sciences, 64*, 496-541.

Day, R.E. (2001). *The Modern Invention of Information: Discourse, History, and Power*. Carbondale, IL: Southern Illinois University Press.

Deibert, R.J. (2002). Circuits of Power: Security in the Internet Environment. In J.N. Roseanna & J.P. Singh (Ed.), *Information Technologies and Global Politics: The Changing Scope of Power and Governance* (pp. 1-38). Albany, NY: State University of New York Press.

Denning, D. (1998). Encryption Policy: Global Challenges and Directions. In H. Ryan & C.E. Pear tree (Ed.), *The Information Revolution and International Security*. Washington, DC: The CSIS Press.

Derrida, J. (1980). *The Archaeology of the Frivolous: Reading Condillac*. Lincoln, NE: University of Nebraska Press.

Deudney, D. (2000). Geopolitics as Theory: Historical Security Materialism. *European Journal of International Relations, 6*. 77-107.

Dhillon, G. & Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. *Information Systems Journal, 11*. 127-153.

Diesing, P. (1991). *How Does Social Science Work?: Reflections on Practice*. Pittsburgh, PA: University of Pittsburgh.

Diken, B. & Lausten, C.B. (2004). 7-11, 9-11, and Postpolitics. *Alternative, 29*. 89-113.

Donovan, G. (2002). Don't Let Security Curtail Refugee Help, Says Official. *National Catholic Reporter, 38*. 6. Retrieved October 5, 2004 from InfoTrac OneFile database.

Dunn, D.D. (2003). Accountability, Democratic Theory, and Higher Education. *Educational Policy, 17*. 60-79.

Earl, M. & Khan, B. (2001). E-Commerce Is Changing the Face of IT. *MIT Sloan Management Review, 43*. 64-77. Retrieved September 22, 2004 from Expanded Academic ASAP database.

Eldred v. Ashcroft, 123 S. Ct. 769 (2003).

Electronic Privacy Information Center. (2002). *Digital Rights Management and Privacy*. Retrieved July 15, 2002, from http://www.epic.org/privacy/drm/

Erlandson, D.A., Harris, E.L., Skipper, B.L. & Allen, S.D. (1993). *Doing Naturalistic Inquiry: A Guide to Methods*. Newbury Park, CA: SAGE Publications.

Etlin, R. (1998). Copyright, Education, and Social Responsibilities. *Historical Journal of Film, Radio, and Television, 18*. 123-128. Retrieved October 9, 2004 from Expanded Academic ASAP database.

Etzioni, A. (1999). *The Limits of Privacy*. New York, NY: Basic Books.

Falkenrath, R.A. (2001). Problems of Preparedness: U.S. Readiness for a Domestic Terrorist Attack. *International Security, 25.* 147-190.

Farmer, D.J. (1995). *The Language of Public Administration: Bureaucracy, Modernity, and Postmodernity*. Tuscaloosa, AL: The University of Alabama Press

Farmer, D.J. (1998). *Papers on the Art of Anti-Administration.* Burke, VA: Chatelaine Press.

Farmer, D.J. (1999). Anti-Admin: With Help From Herbert Marcuse. *Administrative Theory & Praxis, 21*. 497-501.

Farmer, D.J. (2000). The Ladder of Organization-Think: Beyond Flatland. *Administrative Theory & Praxis, 22*. 66-88.

Farmer, D.J. (2002). Constructing Civil Space: A Dialogue. *Administration & Society, 34*. 87-90.

Farmer, D.J. (2002). Public Administration Discourse: A Matter of Style? *Administration & Society, 31*. 299-320.

Farmer, D.J. (2002). Questions. *Administration & Society, 34,* 125-129.

Farmer, D.J. (2002). The Rhetoric of Public Administration. *Administration & Society, 34*. 135-140.

Feinberg, L.E. (2002). Homeland Security: Implications for Information Policy and Practice-First Appraisal. *Government Information Quarterly, 19.* 265-288.

Foster, J.B. (2003). Imperial America and War. *Monthly Review, 55*. Retrieved November 22, 2004, from Expanded Academic ASAP database.

Foucault, M. (1972). *The Archaeology of Knowledge and the Discourse of Language*. New York, NY: Pantheon Books.

Fox, C.J. & Miller, H.T. (1996). *Postmodern Public Administration*. Thousand Oaks, CA: SAGE Publications.

Franda, M. (2002). *Launching into Cyberspace: Internet Development and Politics in Five World Regions*. Boulder, CO: Lynne Reinner Publishers.

Freeman, M. (2003). *Freedom or Security: The Consequences for Democracies Using Emergency Powers to Fight Terror*. Westport, CT: Praeger.

Frisch, D. (1993). Reasons for Framing Effects. *Organizational Behavior and Human Decision Processes, 54*. 399-429.

Galston, W.A. (2002). The Impact of the Internet on Civic Life. In E.C. Kamarck & J.S. Nye (Eds.), *Governance.Com: Democracy in the Information Age* (pp. 40-58). Washington, DC: Brookings Institute.

Garrett, M. & Penny, T.J. (1998). *The Fifteen Biggest Lies in Politics*. New York, NY: St. Martin's Press.

Gertner, Y., Ishai, Y., Kushilevitz, E. & Malkin, T. (2000). Protecting Data Privacy in Private Information Retrieval Schemes. *Journal of Computer and System Sciences, 60*. 592-629).

Glaser, B. & Strauss, A. (1967). *The Discovery of Grounded Theory*. Chicago, IL: Aldine.

Glokany, I.M. (2001). *The Precautionary Principle: A Critical Appraisal of Environmental Risk Assessment*. Washington, DC: CATO Institute.

Golick, J. (2000, February 1). Securing a Multicampus Network. Network Magazine. Retrieved July 22, 2002 from InfroTrac OneFile.

Goold, B.J. (2002). Privacy Rights and Public Spaces: CCTV and the Problem of the "Unobservable Observer." Criminal Justice Ethics, 21. 21-27.

Gregoire, C.O. (2002). Internet Privacy Principles. (Policy Options: Technology). *Spectrum: the Journal of State Government, 75*. 29-31.

Guba, E.G. (1985). The Context of Emergent Paradigm Research. In Y.S. Lincoln (Ed.), *Organizational Theory and Inquiry: The Paradigm Revolution* (pp. 79-104). Beverly Hills, CA: SAGE Publications.

Guba, E.G. & Lincoln, Y.S. (1981). *Effective Evaluation: Improving the Usefulness of Evaluation Results Through Responsive and Naturalistic Approaches*. San Francisco, CA: Jossey-Bass Publishers.

Guba, E.G. & Lincoln, Y.S. (1989). *Fourth Generation Evaluation*. Newbury Park, CA: SAGE Publications.

Gutmann, A. & Thompson, D. (1996). *Democracy and Disagreement*. Cambridge, MA: The Belknap Press of Harvard University Press.

Hager, J.H. (2002, May 30). *Homeland Security National Strategy – Virginia State Document*. Retrieved July 15, 2002 from www.commonwealthpreparedness.state.va.us/documents/ HomelandSecureNatlStrategy.pdf

Halchin, L.E. (2002). Electronic Government in the Age of Terrorism. *Government Information Quarterly, 19*. 243-254.

Halstuk, M.E. & Chamberlin, B.F. (2001). Open Government in the Digital Age: The Legislative History of How Congress Established a Right of Public Access to Electronic Information Held in Federal Agencies. *Journalism & Mass Communication Quarterly, 78*. 45-64.

Harding, S. (1997). Comment on Hekman's "Truth and Method: Feminist Standpoint Theory Revisited": Whose Standpoint Needs the Regimes of Truth and Reality? *Signs, 22*. Retrieved December 1, 2004, from Expanded Academic ASAP database.

Harstock, N. (1987). Rethinking Modernism: Minority vs. Majority Theories. *Cultural Critique, 7*. 187-206.

HB 2211. FOIA: Critical Infrastructure and Vulnerability Assessments. (2003).

Healy, D. (2003). In the Grip of the Python: Conflicts at the University-Industry Interface. *Science and Engineering Ethics, 9*. 59-71.

Hovden, J. (2004). Public Policy and Administration in a Vulnerable Society: Regulatory Reforms Initiated by a Norwegian Commission. *Journal of Risk research, 7*. 629-641.

HR 3162. USA Patriot Act of 2001. 107th Cong., 2nd Session.

H.R. 5005. Homeland Security Act of 2002. 107th Cong., 2nd Session (enacted).

Hult, K.M. & Walcott, C.E. (2001). Separating Rhetoric from Policy: Speechwriting Under Gerald Ford and Jimmy Carter. *White House Studies, 1*. 463-482. Retrieved April 14, 2004, from InfoTrac OneFile database.

Hundleby, C. (1997). Where Standpoint Stands Now. *Women & Politics, 18*. Retrieved December 1, 2004, from Proquest database.

Hutchinson, J.R. (1995). A Multimethod Analysis of Knowledge Use in Social Policy: Research Use in Decisions Affecting the Welfare of Children. *Science Communication, 17*. 90-106.

Hutchinson, J.R. (1996). Using the Role Repertory Grid Technique for Item Generation in a Survey of Knowledge Use. *Journal of Constructivist Psychology, 11*. 149-162.

Huysmans, J. (2002). Defining Social Constructivism in Security Studies: The Normative Dilemma of Writing Security. *Alternatives: Global, Local, Political, 27*. pS41 (22).

Illich, I. (1973). *Tools for Conviviality*. New York, NY: Harper & Row.

Info Management (John Hopkins University Information Security Institute). *R&D, 43,* 13.

Internet of the Future: To Control or be Controlled. *The Futurist, 36,* 27-33.

Israel, C. (2002). The Security Race: Challenges, Leadership and Tools for Success. Retrieved July 19, 2002 from http://www.ta.doc.gov/Speeches?CI_020520_SecurityRace.htm

Jentleson, B.W. (2002). The Need for Praxis: Bringing Policy Relevance Back In. *International Security, 26*. 169-189.

Jordan, T. (2001). Language and Libertarianism: The Politics of Cyberculture and the Culture of Cyberpolitics. *Sociological Review*. 1-17.

Kanner, M.D. (2001). *Desperate Times, Desperate Measures: A Theory of Framing and its Affect on Risk Attitudes*. Unpublished doctoral dissertation, University of Colorado, Boulder.

Kelly, J.D. (2003). U.S. Power, after 9/11 and before it: If not an Empire, Then What? *Public Culture, 15*. 347-369.

Keohane, R.O. & Nye, J.S. (2002) Power and Interdependence in the Information Age. In E.C. Kamarack & J.S. Nye (Eds.), *Governance.Com: Democracy in the Information Age* (pp. 161-178). Washington, DC: Brookings Institute.

Kobrack, P. (1998). Privatization and Cozy Politics. In E.M. Berman, J.P. West & S.J Bonczek (Eds.) *The Ethics Edge*. (pp. 178-192). Washington, DC: ICMA.

Kux, D. (2002). India's Fine Balance. *Foreign Affairs, 81*. Retrieved November 29, 2004, from InfoTrac OneFile database.

Lerner, J.S., Gonzalez, R.M., Small, D.A. & Fischoff, B. (2003). Effects of Fear and Anger on Perceived Risks of Terrorism: A National Field Experiment. *Psychological Science, 14*. 144-150.

Levison, A.B. (1974). *Knowledge and Society: An Introduction to the Philosophy of the Social Sciences*. New York, NY: Pegasus.

Levy, J.S. (2003). Applications of Prospect Theory for Political Science. *Synthese, 135*. 215-241.

Lincoln, Y. & Guba, E. (1985). *Naturalistic Inquiry*. Beverly Hills, CA: SAGE Publications.

Lincoln, Y.S. (1985). The Substance of the Emergent Paradigm: Implications for Researchers. In Y.S. Lincoln (Ed.), *Organizational Theory and Inquiry: The Paradigm Revolution* (pp. 137-157). Beverly Hills, CA: SAGE Publications.

Luke, T.W. (1994). Placing Power/ Siting Space: the Politics of Global and Local in the New World Order. *Environment and Planning D: Society and Space, 12*. 613-628.

Lyotard. (1984). *The Postmodern Condition: A Report on Knowledge*. Minneapolis, MN: University of Minnesota Press.

Majone, G. (1989). *Evidence, Argument and Persuasion in the Policy Process*. New Haven, CT: Yale University Press.

Marshall, C. & Rossman, G.B. (1999). *Designing Qualitative Research, 3rd. Ed.*, Thousand Oaks, CA: SAGE Publications.

Mason, R.O., Mason, F.M. & Culnan, M.J. (1995). *Ethics of Information Management*. Thousand Oaks, CA: SAGE Publications.

MATRIX History. (n.d.). Retrieved March 19, 2004, from http://www.matrix-at.org/history.htm.

McCall, G.J. & Simmons, J.L. (Eds.). *Issues in Participant Observation*. Reading, MA: Addison-Wesley.

McCrohan, K.F. (1998). Competitive Intelligence: Preparing for the Information War. *Long Range Planning, 31*. 586-593.

McGuire, D. (2000, June 19). Official Says US Faces Potential Electronic Pearl Harbor. (National Coordinator for Security, Infrastructure Protection and Counter-Terrorism Richard Clarke). *Newsbytes*. NWSB00172031. Retrieved July 26, 2002 from InfoTrac OneFile database.

Menjivar, C. & Sang, H.K. (2002, Spring/Summer). For Their Own Good: Benevolent Rhetoric and Exclusionary Language in Public Officials' Discourse on Immigrant-Related Issues. *Social Justice*. Retrieved April 14, 2004 from InfoTrac OneFile database.

Miller, H.T. & King, C.S. (1998). Practical Theory. *American Review of Public Administration, 43*. Retrieved from Factiva database: http://global.factiva.com/en/arch/print_results.asp.

Miyazaki, A.D. & Fernandez, A. (2001). Consumer Perceptions of Privacy and Security Risks for Online Shopping. *The Journal of Consumer Affairs, 35*. 27-44.

Morgan, G. (1986). *Images of Organization*. Beverly Hills, CA: SAGE Publications.

Naim, M. (2002/September-October). Post-Terror Surprises: One Consequence of September 11 is the Emergence of a More Sobering, Less Naïve Understanding of Globalization. Foreign Policy. Retrieved November 22, 2004, from Expanded Academic ASAP database.

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission Report: Fianl Report of the National Comission on Terrorist Attacks Upon the United States*. New York: W.W. Norton & Company.

National Institute of Standards and Technology. (2003). *Public Affairs Overview*. Retrieved July 19, 2002 from, http://www.nist.gov/public-affairs/budget/20030verview.htm

National Institute of Standards and Technology. (2003). Technology Administration FY 2003 Budget Overview. Retrieved July 19, 2002 from http://www.nist.gov/public_affairs/budget/2003overview.htm.

National Research Council. (2002). *Making the Nation Safe: The Role of Science and Technology in Countering Terrorism*. Washington, DC: The National Academies Press.

National Strategy to Secure Cyberspace. (2003). Washington, DC: Superintendent of Documents. U.S. Government Printing Office.

Naviakha, G. (1999). Defence Spending: Cost of Fighting Imaginary Enemies. *Economic and Political Weekly, 34*. 1085-1088.

Nehf, J.P. (2003). Recognizing the Societal Value in Information Privacy. *Washington Law Review, 78*. 1-91.

Nelson, L. (2002) Protecting the Common Good: Technology, Objectivity, and Privacy. *Public Administration Review, 62*. 69-73.

Netting, F.E. & O'Connor, M.K. (2003). *Organization Practice: A Social Worker's Guide to Understanding Human Services*. Boston, MA: Allyn & Bacon.

O'Connor, E.S. (2000). Plotting the Organization: The Embedded Narrative as a Construct for Studying Change. *The Journal of Applied Behavioral Science, 36*. 174-192.

Office of Homeland Security. (2002). *National Strategy for Homeland Security*. Washington, DC: Office of Homeland Security.

Olsen, F. (2002). Universities Expand Their Anti-Cyberterrorism Research. *The Chronicle of Higher Education*. Retrieved November 21, 2002 from: http://chronicle.com/daily/2002/06/2002062501t.htm.

O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. *Social Science Computer Review, 19*. 17-31.

O'Neil, R.M. (2003, May/June). Academic Freedom and National Security in Times of Crisis. *Academe*. 21-23.

Ostfield, M.L. (2004). Bioterrorism as a Foreign Policy Issue. *SAIS Review, 24*. 131-146.

Patton, M. (1980). *Qualitative Evaluation Methods*. Beverly Hills, CA: SAGE Publications.

Patton, M.Q. (1990). *Qualitative Evaluation and Research Methods, 2nd Ed*. Newbury Park, CA: SAGE Publications.

Pavleva, J.W. (2004). The Critical State of Shared Governance. *Academe*. Retrieved September 24, 2004 from: http://www.aaup.org'publications/Academe/2002/02ja/02jasco.htm.

Pauchant, T.C. & Mitroff, I.I. (2002). Learning to Cope with Complexity. *The Futurist, 36.* 68-69.

Peterson, M.M. (November 1, 2002). Agencies, companies urged to set guidelines for fighting cyberterrorism. Daily Briefing. Retrieved November 9, 2002 from: http://207.27.3.29/dailyfed/1102/110102tdl.htm.

Phillips, D.J. (1998). The Social Construction of a Secure, Anonymous, Electronic Payment System: Frame Alignment and Mobilization Around Ecash. *Journal of Information Technology, 13*, 273-283.

Porcelli, N., Selby, S., Tantono, W., Bagner, J.& Sonu, C. (2002). Members of Congress DebateNational Identification Cards. *Intellectual Property & Technology Law Journal, 14*. 30-32. Retrieved October 5, 2004 from InfoTrac OneFile database.

Postman, N. (1992). *Technopoly: The Surrender of Culture to Technology*. New York, NY: Alfred A, Knopf.

President's Critical Infrastructure Protection Board. (September 2002). *National Strategy to Secure Cyberspace* [Draft]. Retrieved November 9, 2002 from http://www.whitehouse.gov/pcipb/cyberstrategy-draft.ht.

Raab, J. & Milward, H.B. (2003). Dark networks as problems. *Journal of Public Administration Research and Theory, 13*. 413-439.

Rajagopal, B. (2003). Academic Freedom as a Human Right: A Internationalist Perspective. *Academe, 89*. 25-28.

Ramcharan, B. (2004). Human Rights and Political Risk. *The World Today, 60.* 24-25.

Ravetz, J. (2003). A Paradoxical Future for Safety in the Global Knowledge Economy. *Futures, 35*. 811-827. Retrieved July 2, 2004 from InfoTrac OneFile database.

Rein, M. (1973). *Values, Social Science, and Social Policy: Working Paper No. 21*. Cambridge, MA: Joint Center for Urban Studies of M.I.T. and Harvard.

Rein, M. (1976). *Social Science and Public Policy*. New York, NY: Penguin Press.

Rein, M. (1983). *From Policy to Practice*. Armonk, NY: M.E. Sarpe, Inc.

Relyea, H.C. (2002). The Law: Homeland Security: The Concept and the Presidential Coordination Office—First Assessment. *Presidential Studies Quarterly, 32*. 397-411. Retrieved July 19, 2002 from Proquest Social Science Plus database.

Riley, T.B. (2000). *Electronic Governance and Electronic Democracy: Living and Working in the Wired World*. London, UK: The Commonwealth Secretariat.

Risse, T. (2000). "Let's Argue!": Communicative Action in World Politics. *International Organization, 54*. i1 p1.

Rodwell, M.K. (1998). *Social Work Constructivist Research*. New York, NY: Garland Publishing, Inc.

Rodwell, M.K. & Woody, D. (1994). Constructivist Evaluation: The Policy/Practice Context. In E. Sherman & W.J. Reid (Eds.) *Qualitative Research in Social Work*. New York, NY: Columbia University Press.

Rorty, R. (1982). *Consequences of Pragmatism*. Minneapolis, MN: University of Minnesota.

Rorty, R. (1989). *Contingency, Irony, and Solidarity*. New York, NY: Cambridge Press.

Rorty, R. (1991). *Objectivity, Relativism, and Truth: Philosophical Papers, Volume 1*. New York, NY: Cambridge University Press.

Rorty, R. (1993). Feminism, Ideology, and Deconstruction: A Pragmatist View. *Hypatia, 8*. 96-104. Retrieved October 23, 2004 from InfoTrac OneFile database.

Rorty, R. (1998). *Truth and Progress: Philosophical Papers, Volume 3*. New York, NY: Cambridge University Press.

Rorty, R. (1999). *Philosophy and Social Hope*. New York, NY: Penguin.

Rorty, R. (2002). Fighting Terrorism with Democracy. *The Nation, 275*. i13, 11. Retrieved October 11, 2003 from InfoTrac OneFile database.

Rorty, R. (2002). Worlds or Words Apart? The Consequences of Pragmatism for Literary Studies: An Interview with Richard Rorty. *Philosophy and Literature, 26*. 369-396.

Rorty, R. (2003). American Pride, American Shame. *Chronicle of Higher Education, 49*, B10.

Rorty, R. (2004). Universalist Grandeur, Romantic Depth, Pragmatist Cunning. *Diogenes, 51*. 129-142. Retrieved October 23, 2004 from InfoTrac OneFile database.

Rosin, H. (2002). All Talk – Too Many Words about 9/11. *The New Republic, 227*. 12-13.

Rothkopf, D.J. (2002). Business Versus Terror. *Foreign Policy, 130*. 56-64.

S. 3076. To provide risk sharing and indemnification for government contractors supplying anti-terrorism technology and services, and for other purposes. 107th Cong., 2d Session (2002).

Safir, H. (2003). *Security: Policing Your Homeland, Your State, Your City*. New York, NY: St. Martin's Press.

Saksida, M. (1997). The Information Society in the 21st Century: Converting from Analogue to Digital. *Intl. Inform. & Libr. Rev., 29*. 261-267.

Samuelson, P. (2003). The Constitutional Law of Intellectual Property After Eldred v. Ashcroft. *The Journal of the Copyright Society of the U.S.A., 50*. 547-579.

Sarewitz, D., Pielke, R. & Keykhah, M. (2003). Vulnerability and Risk: Some Thoughts from a Political and Policy Perspective. *Risk Analysis, 23*. 805-810.

Sayegh, F.A. (2004). Post-9/11 changes in the Gulf: the case of UAE. *Middle East Policy, 11*. Retrieved November 29, 2004 from Expanded Academic ASAP database.

Schön, D.A. & Rein, M. (1994). *Frame Reflection: Toward the Resolution of Intractable Political Controversies*. New York, NY: Basic Books.

Schulman, A. (2002, March 30). *The US/Mexico Border Crossing Card (BCC): A Case Study in Biometric, Machine-Readable ID*. Paper presented at the 2002 Conference on Computers, Freedom, and Privacy. Retrieved September 25, 2004 from ACM Portal database.

Schwandt, T.A. & Halpern, E.S. (1988*). Linking Audit and Metaevaluation: Enhancing Quality in Applied Research*. Newbury Park, CA: SAGE Publications.

Seidman, I. (1998). *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences, 2nd Ed*., New York, NY: Teacher's College Press.

Shapiro, A.L. (1999). *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*. New York, NY: PublicAffairs.

Simon, L.D. (2000). *NetPolicy.Com: Public Agenda for a Digital World*. Baltimore, MD: Johns Hopkins University Press.

Singer, M. (2001). The Challenge to Science: How to Mobilize American Ingenuity. In S. Talbott & N. Chanda (Eds.), *The Age of Terror: America and the World After September 11*. New York, NY: Basic Books.

Singh, J.P. (2002). Introduction: Information Technologies and the Changing Scope of Global Power and Governance. In J.N. Roseanau & J.P. Singh (Ed.), *Information Technologies and Global Politics: The Changing Scope of Power and Governance* (pp. 1-38). Albany, NY: State University of New York Press.

Smith, D.E. (1997). Comment on Hekman's "Truth and Method: feminist Standpoint Theory Revisited." *Signs, 22*. Retrieved December 1, 2004, from Expanded Academic ASAP database.

Smith, H.J., Milberg, S.J. & Burke, S.J. (June, 1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*. 167-196.

Smith, M.F. (2001). Pressures on Research and Academic Freedom. *Academe, 87*. 94.

Spight, C. (Presenter). (2000, February 10). Separating Earth from Sky [Video recording]. Richmond, VA: Virginia Commonwealth University.

State Council of Higher Education in Virginia. (2002). *SCHEV's Privacy Statement and Policy*. Retrieved July 15, 2002, from http://www.schev.edu/SCHEVs/privacy.asp.

Stough, R.R., Kulkarni, R. & Trice, M. (2000). *Technology in Virginia's Regions*. Prepared for the Virginia Center for Advanced Technology by the Mason Enterprise Center, The Institute of Public Policy, and George Mason University.

Strickland, L.S. (2002). *Understanding Privacy and the Tension with Security*. Paper presented at the Virginia Library Association Conference, Williamsburg, VA.

Tennyson, R. & Wilde, L. (2000). *The Guiding Hand: Brokering Partnerships for Sustainable Development*. The Prince of Wales Business Leaders Forum and the United Nations Staff College.

Tien, Lee. (2001). Access to Information After 9/11. *Electronic Freedom Foundation*. Retrieved September 25, 2004 from ACM Portal database.

Tierney, W.G. (2003). The University After 9/11. *Qualitative Inquiry, 9*. 325-329.

Tillman, B. (2002). The Changing Political Landscape: the War on Terrorism Delays

Congressional Action on Privacy, the Paperwork reduction Act, and E-Government. *Information Management Journal, 36*. 14-18. Retrieved March 19, 2004 from InfoTrac OneFile database.

Timura, C.T. (2001). "Environmental Conflict" and the Social Life of Environmental Security Discourse. *Anthropological Quarterly, 74*. 104-113.

Torobin, J. (2004). Voice for Privacy In a Chorus of Security. *Congressional Quarterly Weekly Report, 62*. 11.

U.S. Department of Homeland Security. (n.d.) The Privacy Office of the U.S. Department of Homeland Security. Retrieved October 9, 2004 from http://www.dhs.gov/dhspublic/display?theme=content=3961&print=true

V-ONE Corporation Secures the Anti-Terrorism Information Exchange. (2003, July 28). *Business Wire*, 5063.

Vaida, B. (2002, August 5). Panel Endorses Science and Tech Position in Security Agency. *National Journal's Technology Daily*. 1-3. Retrieved November 11, 2002 from http://207.27.3.29/dailyfed/0802/080502njl.htm.

Vaida, B. & Lawson, S.M. (2002, September 18). Administration Unveils Cybersecurity Plan. National Journal's Technology Daily. 1-2. Retrieved November 9, 2002 from http://207.27.3.29'dailyfed/0902/091802tdl.htm.

Virginia's Technology Symposium Comes to Roanoke. (2003). *Virginia Business, 18*. 49-53.

Wagner, C.G. (2001). Securing Our Information. *The Futurist, 35*. 9-12.

Walsham, G. (1990). Organizational Metaphors and Information Systems Research. *European Journal of Information Systems Research, 1*. 83-94.

Walsham, G. (1995). Interpretive Case Studies in IS Research: Nature and Method. *European Journal of Information Systems, 4*. 74-81.

Westin, A.F. (1974). The Technology of Secrecy. In N. Dorsen & S. Gillers (Eds.), *None of Your Business* (pp. . New York, NY: Viking Press.

White, J.D. (1986). On the Growth of Knowledge in Public Administration. *Public Administration Review, 46*. 15-24.

White, J.D. (1992). Knowledge Development and Use in Public Administration: Views

from Postpositivism, Poststructuralism, and Postmodernism. In M.T. Bailey & R.T. Mayer (Eds.), *Public Management in an Interconnected World: Essays in the Minnowbrook Tradition*. New York, NY: Greenwood Press.

White, J.D. (1999). *Taking Language Seriously: The Narrative Foundations of Public Administration Research*. Washington, DC: Georgetown University Press.

Wilber, K. (2000). *A Theory of Everything: An Integral Vision for Business, Politics, Science, and Spirituality*. Boston, MA: Shambala Publications, Inc.

Winant, S. (1999). *Copyright and Libraries*. Paper presented at the Virginia Community College System Learning Resources Peer Group Conference, Richmond, VA.

Wise, C.R. (2002). Organizing for Homeland Security. *Public Administration Review, 62*. 131-144.

Wong, N. (2002). *Critical Infrastructure and Information Assurance: A Working Context and Framework. Security in the Information Age: New Challenges, New Strategies. Compendium of Papers Submitted to the Joint Economic Committee* (Congressional Document No. 79-939, pp. 104-114). Washington, DC: Congress of the United States.

Zahariadis, N. (2003). *Ambiguity and Choice in Public Policy: Political Decision Making in Modern Democracies*. Washington, DC: Georgetown University Press.

Zeller, N. (1987). A Rhetoric of Naturalistic Inquiry. Unpublished doctoral dissertation, Indiana University, Bloomington, IN.

Zeller, N. & Farmer, F. (1999). "Catchy, clever titles are not acceptable" : Style, APA, and qualitative reporting. Qualitative Studies in Education, 12. 3-19.

Appendix A

List of Acronyms

ACLU – American Civil Liberties Union

AOL – America Online

APA – Auditor of Public Accounts

ASIS – American Society of Industrial Security

ATIX – Anti-Terrorism Information Exchange

ATP – Advanced Technology Program

CEO – Chief Executive Officer

CIA – Central Intelligence Agency

CIO – Chief Information Officer

CIPP – Critical Infrastructure Protection Project

CIRT – Computer Incidence Response Team

CISC – Commonwealth Information Security Center

CTEA – Copyright Term Extension Act

CTRF – Commonwealth Technology Research Fund

DARPA – Defense Advanced Research Projects Agency

DC – District of Columbia

DHS – Department of Homeland Security

DMCA – Digital Millennium Copyright Act

DNA – Deoxyribonucleic Acid

DOS – Denial of Service

DRM – Digital Rights Management

DVD – Digital Video Disk

FBI – Federal Bureau of Investigation

FCC – Federal Communications Commission

FERPA – Federal Education Rights and Privacy Act

FOIA – Freedom of Information Act

FSMA – Financial Services Modernization Act

GAO – General Accounting Office

GMU – George Mason University

GW – George Washington University

HIPAA – Health Insurance Portability and Accountability Act

HSPD – Homeland Security Presidential Directive

I3P – Institute for Information Infrastructure Protection

ICT – Information and Communication Technology

IP – Internet Protocol

IS – Information Security

ISAC – Information Sharing and Analysis Center

ISAT – Integrated Science and Technology

ISP – Internet Service Provider

IT – Information Technology

MATRIX – Multi-State Anti-Terrorism Information Exchange

NDIA – National Defense Industrial Association

NIH – National Institutes of Health

NIST – National Institute of Science and Technology

NRA – National Rifle Association

NSF – National Science Foundation

PKI – Public Key Infrastructure

RISS – Regional Information Sharing Systems

ROI – Return on Investment

RPC – Remote Procedure Protocol

SCADA – Supervisory Control and Data Acquisition

SCHEV – State Council of Higher Education in Virginia

SEVIS – Student and Visitor Exchange Information System

SOL – Standards of Learning

SPAM – Self Promotional Advertising Messages

SPIR – Symmetrically-Private Information Retrieval

TIA – Total Information Awareness

TiVo – (Company Name) Personal Video recorder

TV – Television

UCITA – Uniform Computer Information Transactions Act

UK – United Kingdom

US – United States

VASCAN – Virginia Alliance for Secure Computing and Networking

Appendix B

Glossary of Methodological Terms

audit. The process by which the constructivist rigor of trustworthiness and authenticity is attested to by an outside review of the audit trail.

authenticity. Dimension of constructivist research rigor focusing on the quality of the research process, rather than on the research product. Composed of fairness, ontological, educative, catalytic, and tactical aspects.

case report. Preferred method of presenting the results of a constructivist study, usually written in a narrative style and providing a thick description of the phenomena under investigation, the context of the investigation, and the results of the co-construction by inquiry participants. *See also* case study.

case study. Generally interchangeable with the case report as the primary vehicle for emic inquiry that builds on the reader's tacit knowledge and allows for reader judgment regarding transferability of the information to another known context. *See also* case report.

catalytic authenticity. A measure of constructivist research rigor that demonstrates that change or reshaping has resulted from the research process. *See also* authenticity.

co-construction. In relational conversation, the dialogic and dialectical process by which research participants, together with the inquirer, create a reality and share an understanding of it.

confirmability. A measure of constructivist research that demonstrates that research results are linked to the data collected during the inquiry. *See also* trustworthiness.

constructed reality. What exists in the minds of individuals; a cognitive process that leads to an infinite number of constructions and, hence, multiple realities; reality is constructed through the use of some common referent terms that could be understood (constructed) differently by different individuals.

constructivism. A philosophical framework and an approach to research that assumes that reality is constructed, based on intersubjectively achieved meaning that cannot generalize beyond the time and context of the encounter; that there are no fundamental causes, but instead networks of relationships that produce multiple and simultaneous shaping to the construction of reality. Focus is on cognitive schemas that construct the subject's experience and action and lead to new interpretive frameworks or structures.

contextual reality. A type of constructed reality absolutely imbedded in the particulars of a given situation or environment.

credibility. A measure of constructivist research rigor that demonstrates the findings are believable. *See also* trustworthiness.

dependability. A measure of constructivist rigor that demonstrates that the procedures used to gather, analyze, and interpret data fall within accepted constructivist practices. *See also* trustworthiness.

dialectic. Process of meaning making when meaning relations are oppositional, dual, contradictory, or arbitrary; can involve the uniting of opposites into a new totality such as in the synthesis of a thesis and antithesis.

discourse. A focused discussion, usually formal and based on reason, with the aim of communication and study.

educative authenticity. A measure of constructivist research rigor that demonstrates there was increased understanding of and respect for the value systems of others as a result of the inquiry process. *See also* authenticity.

emergence. Describes a research design that allows an orderly development of an inquiry based on what comes forth from the context and process without determining the structure and process beforehand.

emic. Providing an insider's view or perspective.

etic. Providing an outsider's perspective.

fairness. A measure of constructivist rigor that demonstrates that there is an evenhanded representation of all viewpoints throughout the research process and in the research product. *See also* authenticity.

gatekeeper. A person who, by virtue of position, power, or expertise can provide or prevent access to information or sources of information.

generalizability. The ability of a truth to hold across time and circumstance.

grounded theory. An explanation or a description of a phenomenon that results as data emerge and are analyzed.

hermeneutic circle. A circular conversation among and between interested parties (including relevant texts), wherein perspectives and insights are shared, tested, and evaluated. *See also* hermeneutic dialectic.

hermeneutic dialectic. The process within the hermeneutic circle by which perspectives are compared and placed in contradiction so that, through testing and evaluation, a higher level of sophistication can be achieved, generally filled with, at least, tension, if not conflict. *See also* hermeneutic circle.

ideographic. Having the nature of a graphic symbol that represents an object or idea, rather than a word used for the same purpose.

idiographic. Descriptions or interpretations that are unique to the individual, that capture what is individually distinctive.

induction. A reasoning process moving from lower to higher levels of abstraction, going from the particular to the general.

inquiry context. The physical and psychological backdrop for the research undertaking; the location in which the research is taking place.

interpretive paradigm. A perspective informed by a concern to understand the world as it is at the level of subjective experience, within the realm of individual consciousness and subjectivity, and from the frame of reference of the participant, as opposed to the observer.

meaning construction. Based on the assumption of a socially constructed reality. It is the communication process through which understanding between individuals and perspectives is achieved by creating relational ties between one item or concept and another with word or symbolic interpretations.

member check. Major activity of constructivist rigor of both trustworthiness and authenticity, whereby the inquiry respondents are asked to warrant that what has been understood or produced is an accurate reflection of their reality.

minority report. In recognition of multiple realities and the difficulty of gaining consensus through hermeneutic dialectic, the presentation of the claims, concerns, or issues of those for whom consensus was not possible. It is in the form of an addendum to the final constructivist report.

multiple causality. Simultaneous influencing of factors over time in such a way that it is no longer relevant to ask which caused which, sometimes known as mutual causality or mutual simultaneous shaping, because everything influences everything else, in the here and now.

multiple meanings. In constructivism, the assumption that each individual will construct his or her understanding of experience and action, and that even individuals having the same experience will invent different interpretive frameworks or structure to understand, so that the number of interpretations will match the number of individuals having the experience.

multiple perspectives. In constructivism, the assumption that our perspectives affect what we see, so that any one focus of observation only gives a partial result. In order to hope to achieve a complete picture, many points of view are required. To control biases and develop more than a partial understanding, a plurality of kinds of knowledge must be explored by a multiplicity of methods.

naturalistic research. Within the positivist perspective, the systematic study of a phenomenon in its context, without intentional alteration for research purposes. In the interpretive perspective, the original title of what is now known as constructivist research.

negotiated outcomes. The required results of a constructivist inquiry. Meaning, interpretations, and the final product must be negotiated with the human sources because it is their construction of

reality, and because participants own their own data. The goal of the negotiation is accurate reconstruction of perspectives.

ontological authenticity. A measure of constructivist research that demonstrates increased awareness of the complexity of the phenomenon under investigation. *See also* authenticity.

ontology. Perspective on the nature of reality. Is it above and beyond individual knowledge or is it based on individual consciousness, apart from the outside world?

paradigm. How one orders reality: the general organizing principles governing perceptions including beliefs, values, techniques used to describe what exists, where to look, and what scientists expect to discover. It is a worldview with a set of axioms and systems, all related to one another for discipline inquiry.

paradox. Holding seemingly contradictory opinions, interpretations, or two different things true at the same time.

peer debriefing. As a part of peer review, the process whereby the peer reviewer poses searching questions in order to help the researcher understand his or her own perspective and behavior in the research process, and test working hypotheses outside the inquiry context to enhance the emergent design.

peer review. The process in constructivist research whereby an outside agent or reviewer is engaged to accompany the research process in order to discuss feelings, findings, and conclusions in a process that resembles clinical supervision. *See also* peer debriefing.

qualitative methods. The preferred means of collecting data in constructivist research because of their adaptability to multiple realities and because they expose, more directly, the nature of the transaction between investigator and participant. They allow for easier access to the biases of the investigator and are more sensitive to mutual shaping and influences. The preferred qualitative methods in constructivism are: interviews, participant observations, and focus groups.

quantitative methods. The preferred means of collecting data in traditional research in the positivist and post-positivist perspective because of the assumed ability to control intersubjectivity and other biasing effects that could hamper generalizability. Preferred quantitative methods are use of standardized instruments within a controlled research design.

radicalism. Favoring fundamental change of the center, foundation, or source as in the social structure. Generally seen to be extreme, mostly used to describe leftist political preferences, as opposed to conservative preferences.

rationalization. To explain or interpret on rational grounds. Usually meant to describe a process in which superficially rational or plausible explanations or excuses are devised to support one's acts, beliefs, or desires without one's being aware that these are not real motives.

reactivity. Responding to stimulus, to be affected by some influence, event, or experience.

reconstruction. The last step in constructivist data analysis after unitizing (a deconstructive process) whereby, through categorizing all data with a constant comparison of one unit to another, the material is brought together in a new and, hopefully, more meaningful way.

reductionism. The philosophical assumption that we achieve a better understanding of anything after we have broken down formal and final cause theoretical conceptions to underlying material and efficient cause theoretical conceptions. This is a "building block" conception of reality where little unities constitute bigger totalities and the goal is to reduce everything to the substrata that make them up. *See also* cause.

reflexive journal. During the constructivist inquiry process, a required dimension of trustworthiness that reports on the inquirer's progressive bounding of subjectivity, in which reflections are made regarding inner biases and conflicts, and the strategies devised that are used to cope with or resolve these barriers to understanding. The journal should chronicle the development of different or deeper insights and understandings of the context and perspectives of the inquiry participants.

reflexivity. The ability of the human mind to turn back on itself and, therefore, know that it is knowing.

relativism. A perspective on knowledge which maintains that the basis of judgment and/ or knowing is relative, differing according to events, persons, etc.

rhetoric. The use of words effectively in speaking or writing to influence or persuade.

rigor. All aspects of the demonstration of quality in constructivist research including trustworthiness, negotiated outcomes, authenticity, and the quality of the hermeneutic circle.

schema. In constructivism, the cognitive map or diagram that serves to represent something, principally the result of the data analysis process, but can also refer to the way individuals categorize to make sense out of complexity.

stakeholder. An individual with a vested interest. In research, stakeholders are all individuals with a perspective or with something to gain or lose, as a result of the process or product of inquiry.

subjectivity. Refers to constructs with meanings that are personal and, therefore, incapable of being extended beyond the individual who has framed the meaningful relationship intended. Subjective meanings cannot be totally understood, even when we sincerely examine the contents at issue, because social reality exists primarily in the individual's consciousness or mind.

tacit knowledge. Intuitions, feelings that have not yet taken prepositional (language) form. Something cannot be stated, but it is somehow known to be the subject.

tactical authenticity. A measure of constructivist research rigor that demonstrates empowerment or redistribution of power among stakeholders supportive of effective change. *See also* authenticity.

theory. A series of two or more schematic labels (words, symbols, concepts, etc.) that have been hypothesized, presumed, or demonstrated to bear a meaningful relationship with one another.

theory building. The process by which the relationship between concepts is described.

theory testing. The process by which the relationship between concepts is proven or disproved.

transferability. A measure of constructivist research rigor that demonstrates sufficient information about the context and the phenomenon under investigation has been provided in the final product, the case report, to allow the reader to make judgments about similarities of the findings with other contexts. *See also* trustworthiness.

triangulation. Using different modes of data collection to cross-check data collected and data analyzed.

trustworthiness. The constructivist criteria for testing the rigor of constructivist studies, paralleling the criteria for rigor found in traditional research. It includes credibility (analogous to internal validity), dependability (analogous to reliability), confirmability (analogous to objectivity), and transferability (analogous to external validity).

truth. A fact or reality related to actual existence and able to be verified. In traditional science it must also be established to exist across time and context.

values. Those things that are desirable or worthy of esteem for their own sakes. That which is intrinsic worth and is regarded in a particularly favorable way.

Note. From Social Work Constructivist Research (pp. 253-263), by M.K. Rodwell, 1998, New York, NY: Garland Publishing, Inc. Adapted with permission.

Appendix C

Research Subject Information and Consent Form

Title: Security, Technology, and Public Policy: A Constructivist Inquiry

VCU IRB Protocol Number:

Sponsor:

Investigator: Mary Katherine O'Connor
Linda F. Larkin, Ph.D. Candidate, Public Policy and Administration

Purpose of the Study:
The purpose of this study is to 1) satisfy dissertation requirements for the Doctor of Philosophy in Public Policy and Administration and 2) explore the discourse surrounding public policy development, security, and technology.

Description:
This research into information security policy development will include questions about your perceptions of the policy development process, the meaning of security, and the role technology and technological language play. The study is a constructivist inquiry meaning that it uses qualitative methods to better understand the subjective experiences of participants. Your participation will begin with a one hour face-to-face interview and at least one short follow-up interview, as well as for member checks. Member checks will give you the opportunity to clarify your responses and may involve reading parts of the case study report that will be written about various understandings of the topic. Member checks will last no longer than 30 minutes and may be as brief as 5 minutes.

There will be no more than 75 participants in this study. Participants will represent a wide range of stakeholders in information security policy development within higher education institutions in Virginia.

Procedures:
If you decide to participate in this research, you will be asked to sign this consent form after you have had all your questions answered.

Risks and Discomforts:
The nature of the questions in this study, dealing with issues of security and technology in policy-making is not likely to cause participants either physical or emotional discomfort. However, it is not unusual for an inquiry of this kind to present new ways of thinking about a phenomenon and the questioning of one's beliefs can be stressful.

Voluntary Participation and Withdrawal:
While it is hoped that your participation will continue throughout the course of this research, you may choose to withdraw at any time. Choosing not to participate will not have any negative consequences for you or the agency you represent.

Confidentiality:
Your identity will be treated with professional standards of confidentiality. Your identity will not be revealed as information is shared with other participants or in any subsequent publication of this study. All field notes and records will be coded with identifying numbers and kept in a secure area. No identifying information will be used to connect you to your identification number at any stage of the research process. Access to the research data is limited to the principal investigator and the dissertation committee.

Compensation for Injury:
In the event of physical and/or mental injury resulting from your participation in this study, Virginia Commonwealth University/MCV Hospitals will not provide compensation. If injury occurs, contact your doctor immediately. Fees for such treatment will be billed to you or the appropriate third party insurance.

Questions:
In the future, you may have questions about your study participation. If you have questions, you may contact the principal investigator, Linda Larkin, M.S., at (540) 898-3939, or Mary Katherine O'Connor, Ph.D., at (804) 828-0688. If you have questions about your rights as a research participant, you may contact the VCU Committee on the Conduct of Human Research at (804) 828-0868.

Consent:
I have read the consent form and understand the information about this study. All my questions have been adequately answered. I understand that I will receive a signed and dated copy of this consent form for my records.

By signing this consent form I have not waived any of the legal rights, which I otherwise would have as a subject in a research study.

Participant's Name (Printed)

Participant's Name (Signed)

Date

Appendix D

Category Sets with Decision Rules and Codes

I. *What are you trying to do?* : This category includes data relating to mission and desired outcome.

a. Roles of the University

1. Traditional – subcategory includes all that relates to traditional roles for colleges and universities
2. Partnerships – subcategory includes all that relates to partnerships between universities and government and/ or industry
3. Consortiums – subcategory includes all that relates to partnerships among colleges and universities

b. Mandates – subcategory includes all that relates to legal mandates to which colleges and universities must adhere

1. Legal issues – subcategory includes all that relates to problems with compliance

c. Protection – subcategory includes all that relates to protection in general

1. subcategory includes all that relates to measures taken to protect records
2. subcategory includes all that relates to safety of students, faculty, and staff

d. Critical Infrastructure – subcategory includes all that relates to critical infrastructure protection

e. Interplay of Technology and Security

1. Human Factor - subcategory includes all that relates to humans and technology and/ or security

f. Educating Users - subcategory includes all that relates to training users in securing their computers

g. Change – subcategory includes all that relates to fear of change or preparing people for change

h. Experts – subcategory includes all that relates to the role of experts

II. *Security and Technology Issues*

a. Issues of Access

1. Open environment v. Security of Data – subcategory includes all that relates to open access v. security of information

a. Data Collection - subcategory includes all that relates to collecting data in a too open or too closed environment

b. Liability – subcategory includes all that relates to access and liability

c. Private sector interests – subcategory includes all that relates to access and private sector interests

b. Security Programs/ Policy - subcategory includes all that relates to elements to security programs and policies

c. Technology - subcategory includes definitions of technology and all that relates to the meanings of technology

1. Using Technology for Security – subcategory includes all that relates to technological security applications
2. Legislation – subcategory includes all that relates to laws relating to technology and/ or security and resulting issues
3. Problems - subcategory includes all that relates to problems and dilemmas involved with implementation of information security policy

d. Risk Assessment - subcategory includes all that relates to the formal process of risk assessment

1. Disaster/ Crisis Planning and Management - subcategory includes all that relates to disaster and/ or crisis planning
2. Return on Investment and Cost/ Value - subcategory includes all that relates to money in relation to risk

e. Protecting information as it is disseminated - subcategory includes all that relates to specific issues related to protecting information that is only valuable if used or disseminated.

1. Deterrents - subcategory includes all that relates to technological applications to protect information as it is used
2. "Building In" Security - subcategory includes all that relates to the embedding of security features in software as opposed to patches
3. Audits - subcategory includes all that relates to elements of auditing process and complying with audits
4. Standards - subcategory includes all that relates to development and compliance with state standards
    a. Subcategory includes all that relates to standard related problems for colleges and universities
5. Developing Security Policy - subcategory includes all that relates to best practices in policy development
6. Changing Role of Security - subcategory includes all that relates to changes in security and policy since 9/11 and/ formation of the Department of Homeland Security

f. Threats – subcategory includes all that relates to the nature of perceived threats

III. *Language and Framing* – subcategory includes all that relates to the importance of the use of language and the manner in which information is presented

a. Perception - subcategory includes all that relates to perception and perspective

b. Who does the framing? - subcategory includes all that relates to who is included in framing issues
    1. Reliance on Framing of Others - subcategory includes all that relates to policy makers relying on others to frame the issues
        a. Lobbying
        b. Advising
        c. Media
c. Spinning/ Marketing - subcategory includes all that relates to varying ways of presenting information
d. Context - subcategory includes all that relates to the importance of context in how issues are framed
e. Reflection - subcategory includes all that relates to reflecting or thinking about the issues or process
f. Policy Making Process - subcategory includes all that relates to how policy is made
    1. Bad Decisions - subcategory includes all that relates to poor policy making
    2. Holistic View - subcategory includes all that relates to systems analysis and seeing the big picture
    3. What is the policy Question? - subcategory includes all that relates to determining what the policy question is
g. Kids - subcategory includes all that relates to kids, children, and/ or the younger generation
    1. Filtering – subcategory includes all that relates to Internet filtering
h. Framing and legislation - subcategory includes all that relates to policy or law resulting from specific framing
i. Language - subcategory includes all that relates to language
    1. Technological Language - subcategory includes all that relates to language and technology
        a. Technology Policy - subcategory includes all that relates to the use of technological language in policy development
j. Stakeholders - subcategory includes all that relates to those affected by the way a law or policy is framed
k. Security - subcategory includes all that relates to definitions of security

IV. *Balance and Trade-Offs* - subcategory includes all that relates to issues of individual freedoms in relation to public safety
a. Information Sharing – subcategory includes all that relates to government and/ or business databases containing personal information
b. Protecting Core Liberties - subcategory includes all that relates to protecting core liberties as opposed to trade-offs
c. Heightened Awareness - subcategory includes all that relates to all that relates to temporary tightening of security

d. Multiple Perspectives - subcategory includes all that relates to importance of finding out what people think
    1. Buy In of Citizens - subcategory includes all that relates to involvement of citizens and their confidence in policy makers
e. International Relations – subcategory includes all that relates to relations between U.S. and other countries
    1. Foreign Students - subcategory includes all that relates to the rights and treatment of foreign students
    2. Exaggerated Risk - subcategory includes all that relates to development of policy in response to exaggerated risk scenarios

Academic Freedom

    3. Universities and Political Pressure - subcategory includes all that relates to government and/ or business influencing university policy
    4. Manipulating Fear - subcategory includes all that relates to deliberate distortion of facts to manipulate results
f. Disclosure – subcategory includes all that relates to balance of full disclosure and secrecy
g. Sharing and Trust - subcategory includes all that relates to working and developing policy in an open environment
    1. Hacker Culture - subcategory includes all that relates to the pros and cons of hacker culture
    2. Organic Information System - subcategory includes all that relates to the importance the interconnectedness and sharing.
    3. Technology and Human Learning - subcategory includes all that relates to human learning as the purpose of technology

Appendix E

What follow are the notes that refer to the raw data source for each reference in the case study. Each note includes one or more data unit. Each data unit is numbered and filed for easy accessibility. The first unit number refers to the order of the interview in relation to the other interviews. The second numeral in the note refers to the order of interviews with a specific participant. The letters refer to initials representing that participant and the final number indicates the number of the unit within an interview set.

Raw Data for Audit Trail

1. 21.1-AM-13; 18.1-NW-3; 1.1-LH-49; 24.1-JD-13; 18.1-NW-4; 18.1-NW-29; 24.1-JD-14; 21.1-AM-24; 21.1-AM-16; 1.1-LH-50; 1.1-LH-51; 9.1-PL-46; 5.1-CG-41; 5.1-CG-42; 18.1-NW-32; 3.1-JP-37.

2. 1.1-LH-33; 18.1-NW-27; 21.1-AM-28; 2.1-BW-12; 14.1-LS-14; 5.1-CG-6; 5.1-CG-7; 5.1-CG-8; 5.1-CG-9; 5.1-CG-10; 3.1-JP-6; 3.1-JP-7; 3.1-JP-8; 3.1-JP-30; 19.1-LN-1; 9.1-PL-19; 1.1-LH-1; 3.1-JP-59; 24.1-JD-3; 12.1-RM-72; 12.1-RM-83; 18.1-NW-71; 6.1-TD-10.

3. 11.1-AG-22; 11.1-AG-23; 11.1-AG-24; 11.1-AG-25; 11.1-AG-23-A.

4. 8.1-KW-42; 8.1-KW-36; 8.1-KW-37; 8.1-KW-43; 8.1-KW-40; 8.1-KW-418.1-KW-44.

5. 9.1-PL-30; 9.1-PL-32; 9.1-PL-33; 9.1-PL-34; 9.1-PL-35; 9.1-PL-36; 9.1-PL-37; 9.1-PL-38.

6. 4.1-MI-1; 6.1-TD-7; 4.1-MI-2; 6.1-TD-8; 4.1-MI-13; 4.1-MI-14.

7. 11.1-AG-30.

8. 11.1-AG-1; 11.1-AG-2; 11.1-AG-3; 11.1-AG-4.

9. 16.1-JH-11.

10. 19.1-LN-21; 19.1-LN-22; 19.1-LN-23.

11. 23.1-SP-4; 3.1-JP-44; 3.1-JP-46; 3.1-JP-47.

12. 7.1-RM-5; 7.1-RM-2; 7.1-RM-3.

13. 4.1-MI-57; 4.1-MI-15.

14. 5.1-CG-11; 5.1-CG-12; 7.1-RM-11; 3.1-JP-29; 16.1-JH-10; 2.1-BW-50; 14.1-LS-5; 14.1-LS-6.

15. 14.1-LS-7.

16. 7.1-RM-10; 17.1-JH-7; 24.1-JD-19; 23.1-SP-2; 5.1-CG-5; 23.1-SP-3; 5.1-CG-40; 24.1-JD-4; 1.1-LH-4; 18.1-NW-6.

17. 24.1-JD-16; 20.1-JS-10; 1.1-LH-5; 14.1-LS-9; 24.1-JD-5; 24.1-JD-6; 24.1-JD-7; 24.1-JD-8; 24.1-JD-9; 17.1-JH-1.

18. 12.1-RM-26.

19. 6.1-TD-11.

20. 19.1-LN-20.

21. 3.1-JP-9; 3.1-JP-10; 3.1-JP-11; 3.1-JP-57; 3.1-JP-58; 10.1-RP-12; 25.1-BV-31; 3.1-JP-12; 5.1-CG-15; 4.1-MI-56.

22. 9.1-PL-44; 12.1-RM-84; 11.1-AG-29; 6.1-TD-35; 2.1-BW-29; 5.1-CG-32; 9.1-PL-45; 12.1-RM-85.

23. 18.1-NW-62; 18.1-NW-63; 18.1-NW-64.

24. 12.1-RM-4.

25. 13.1-JL-8.

26. 21.1-AM-30.

27. 20.1-JS-7; 10.1-RP-11; 12.1-RM-38; 14.1-LS-47; 10.1-RP-16; 24.1-JD-23; 14.1-LS-46; 4.1-MI-47; 20.1-JS-8.

28. 24.1-JD-12; 10.1-RP-15; 24.1-JD-22; 7.1-RM-12.

29. 15.1-JH-22; 3.1-JP-25;

30. 4.1-MI-5; 5.1-CG-38; 15.1-JH-19.

31. 12.1-RM-35.

32. 18.1-NW-49.

33. 13.1-JL-4; 13.1-JL-5; 13.1-JL-6.

34. 5.1-CG-39; 16.1-JH-12; 23.1-SP-25; 17.1-JH-14; 7.1-RM-53; 7.1-RM-1; 22.1-AC-10; 1.1-LH-39; 7.1-RM-25; 20.1-JS-24; 7.1-RM-49; 21.1-AM-33; 7.1-RM-7; 19.1-LN-32; 10.1-RP-17.

35. 4.1-MI-42.

36. 21.1-AM-64.

37. 23.1-SP-1.

38. 14.1-LS-36; 19.1-LN-49; 19.1-LN-43; 19.1-LN-44; 19.1-LN-46; 19.1-LN-47; 19.1-LN-48; 18.1-NW-95.

39. 15.1-JH-4; 15.1-JH-8; 15.1-JH-9.

40. 9.1-PL-30-A; 9.1-PL-31.

41. 18.1-NW-46.

42. 15.1-JH-5; 15.1-JH-6; 20.1-JS-25.

43. 20.1-JS-23; 20.1-JS-26.

44. 7.1-RM-51.

45. 14.1-LS-57; 23.1-SP-33; 21.1-AM-68; 21.1-AM-69; 21.1-AM-67-A.

46. 21.1-AM-70.

47. 21.1-AM-1; 21.1-AM-2; 21.1-AM-8.

48. 12.1-RM-44; 12.1-RM-45; 12.1-RM-46; 12.1-RM-47; 12.1-RM-30; 12.1-RM-78; 10.1-RP-21; 10.1-RP-13; 10.1-RP-20; 6.1-TD-72; 12.1-RM-53; 12.1-RM-54.

49. 5.1-CG-82; 5.1-CG-74; 5.1-CG-75; 5.1-CG-76; 5.1-CG-77; 5.1-CG-78; 5.1-CG-79; 5.1-CG-80; 5.1-CG-81; 5.1-CG-83.

50. 19.1-LN-2; 19.1-LN-5.

51. 9.1-PL-6; 9.1-PL-7; 9.1-PL-8; 12.1-RM-36.

52. 24.1-JD-43; 24.1-JD-49; 24.1-JD-44; 24.1-JD-45; 24.1-JD-4624.1-JD-47.

53. 7.1-RM-48; 5.1-CG-2.

54. 9.1-PL-4; 15.1-JH-26.

55. 12.1-RM-50; 12.1-RM-51; 12.1-RM-52.

56. 24.1-JD-31; 24.1-JD-48; 9.1-PL-5; 20.1-JS-11; 16.1-JH-6.

57. 14.1-LS-54; 14.1-LS-55.

58. 12.1-RM-55; 12.1-RM-56; 12.1-RM-57; 12.1-RM-58.

59. 12.1-RM-75; 12.1-RM-59.

60. 7.1-RM-38; 12.1-RM-29.

61. 12.1-RM-60.

62. 3.1-JP-32; 3.1-JP-33; 3.1-JP-34.

63. 5.1-CG-45; 5.1-CG-46; 5.1-CG-47; 5.1-CG-85.

64. 24.1-JD-15; 6.1-TD-31; 24.1-JD-39; 23.1-SP-17.

65. 7.1-RM-30; 10.1-RP-10; 24.1-JD-10; 5.1-CG-19; 3.1-JP-16; 3.1-JP-17; 3.1-JP-18; 3.1-JP-19; 3.1-JP-20; 3.1-JP-21; 14.1-LS-16; 14.1-LS-17; 23.1-SP-5; 23.1-SP-6; 23.1-SP-7; 23.1-SP-8; 23.1-SP-9; 23.1-SP-10; 23.1-SP-11; 23.1-SP-12; 9.1-PL-2; 10.1-RP-9; 1.1-LH-47; 17.1-JH-4; 19.1-LN-10; 19.1-LN-11; 18.1-NW-39; 18.1-

NW-40; 18.1-NW-41; 18.1-NW-42; 5.1-CG-20; 5.1-CG-21; 5.1-CG-22; 5.1-CG-23; 5.1-CG-24; 5.1-CG-25; 5.1-CG-26; 2.1-BW-15; 2.1-BW-16; 2.1-BW-17; 2.1-BW-18; 2.1-BW-27; 11.1-AG-20; 11.1-AG-33; 15.1-JH-10; 16.1-JH-8; 5.1-CG-27; 2.1-BW-19; 2.1-BW-20; 2.1-BW-24; 2.1-BW-25; 2.1-BW-26; 2.1-BW-28; 14.1-LS-53; 22.1-AC-7; 20.1-JS-4; 20.1-JS-5.

66. 24.1-JD-20; 24.1-JD-25; 21.1-AM-19.

67. 10.1-RP-8; 21.1-AM-20; 21.1-AM-21; 21.1-AM-22; 8.1-KW;17; 21.1-AM-31; 10.1-RP-22.

68. 19.1-LN-6; 7.1-RM-6; 6.1-TD-9; 22.1-AC-5; 19.1-LN-31; 23.1-SP-51; 17.1-JH-3; 6.1-TD-27; 6.1-TD-28; 6.1-TD-29; 6.1-TD-30; 2.1-BW-13; 2.1-BW-21; 2.1-BW-22; 2.1-BW-23; 3.1-JP-13; 3.1-JP-14; 24.1-JD-24.

69. 23.1-SP-13; 23.1-SP-14; 23.1-SP-15; 23.1-SP-16; 25.1-BV-24; 25.1-BV-25; 25.1-BV-26; 25.1-BV-22; 25.1-BV-23.

70. 25.1-BV-27; 19.1-LN-12; 1.1-LH-30; 25.1-BV-32.

71. 3.1-JP-22; 1.1-LH-29; 20.1-JS-6; 24.1-JD-21.

72. 15.1-JH-21; 11.1-AG-21; 7.1-RM-31; 5.1-CG-30; 5.1-CG-28; 6.1-TD-68.

73. 22.1-AC-2; 22.1-AC-3.

74. 7.1-RM-20; 1.1-LH-9; 13.1-JL-22.

75. 19.1-LN-52; 7.1-RM-16; 12.1-RM-33; 12.1-RM-96.

76. 19.1-LN-45.

77. 7.1-RM-17; 7.1-RM-18; 7.1-RM-19.

78. 1.1-LH-35; 1.1-LH-36; 1.1-LH-37; 1.1-LH-42; 1.1-LH-38; 7.1-RM-23.

79. 22.1-AC-6; 22.1-AC-12.

80. 18.1-NW-52; 18.1-NW-53; 18.1-NW-54; 15.1-JH-18.

81. 14.1-LS-22; 14.1-LS-11; 10.1-RP-57.

82. 16.1-JH-13.

83. 12.1-RM-61; 12.1-RM-62; 12.1-RM-63; 12.1-RM-64; 12.1-RM-65; 12.1-RM-66; 12.1-RM-67; 1.1-LH-43.

84. 6.1-TD-69.

85. 12.1-RM-68.

86. 10.1-RP-25; 23.1-SP-52; 23.1-SP-53; 7.1-RM-21; 10.1-RP-24; 10.1-RP-26; 10.1-RP-27; 23.1-SP-57.

87. 14.1-LS-18; 14.1-LS-13; 14.1-LS-157; 7.1-RM-9; 14.1-LS-19.

88. 15.1-JH-17; 5.1-CG-49; 5.1-CG-18.

89. 6.1-TD-39; 19.1-LN-33; 6.1-TD-40; 19.1-LN-38; 19.1-LN-41; 19.1-LN-35; 6.1-TD-23.

90. 7.1-RM-52; 12.1-RM-37.

91. 16.1-JH-9; 15.1-JH-23; 18.1-NW-18; 18.1-NW-10; 18.1-NW-11; 18.1-NW-2; 18.1-NW-7; 18.1-NW-8; 18.1-NW-9; 19.1-LN-50; 1.1-LH-6; 15.1-JH-25.

92. 22.1-AC-11.

93. 18.1-NW-13.

94. 21.1-AM-44; 20.1-JS-13; 24.1-JD-26.

95. 14.1-LS-24; 21.1-AM-27.

96. 1.1-LH-17; 3.1-JP-54; 3.1-JP-55; 20.1-JS-2; 5.1-CG-29; 1.1-LH-3; 1.1-LH-13; 1.1-LH-14; 1.1-LH-15; 1.1-LH-16; 1.1-LH-22; 1.1-LH-24; 1.1-LH-18; 1.1-LH-19; 1.1-LH-20; 1.1-LH-21; 1.1-LH-23; 5.1-CG-86.

97. 12.1-RM-5-A; 12.1-RM-6; 12.1-RM-90; 12.1-RM-8; 12.1-RM-89.

98. 16.1-JH-724.1-JD-28; 24.1-JD-29; 24.1-JD-53; 14.1-LS-37.

99. 12.1-RM-9; 6.1-TD-17; 20.1-JS-3; 20.1-JS-14; 14.1-LS-44; 14.1-LS-45.

100. 6.1-TD-18.

101. 18.1-NW-5.

102. 12.1-RM-14-A; 12.1-RM-7; 12.1-RM-31; 12.1-RM-80; 12.1-RM-81; 6.1-TD-32; 6.1-TD-26; 12.1-RM-86; 12.1-RM-76; 12.1-RM-77; 22.1-AC-10-A; 22.1-AC-8; 22.1-AC-9; 6.1-TD-16.

103. 16.1-JH-29.

104. 24.1-JD-51; 24.1-JD-54; 24.1-JD-50.

105. 23.1-SP-32.

106. 18.1-NW-16; 18.1-NW-17; 18.1-NW-12; 6.1-TD-34.

107. 9.1-PL-17.

108. 18.1-NW-25; 18.1-NW-58.

109. 18.1-NW-24; 18.1-NW-57.

110. 7.1-RM-24; 7.1-RM-4; 18.1-NW-14; 18.1-NW-15.

111. 18.1-NW-51.

112. 18.1-NW-56; 3.1-JP-60; 3.1-JP-36.

113. 12.1-RM-18; 12.1-RM-19; 12.1-RM-20; 6.1-TD-6; 23.1-SP-26; 23.1-SP-27; 10.1-RP-14; 24.1-JD-18; 2.1-BW-14; 12.1-RM-87; 12.1-RM-88; 1.1-LH-31; 6.1-TD-33; 1.1-LH-12.

114. 6.1-TD-13; 12.1-RM-15; 12.1-RM-16; 12.1-RM-17; 12.1-RM-10; 12.1-RM-11; 12.1-RM-12; 12.1-RM-13; 7.1-RM-41.

115. 12.1-RM-14.

116. 6.1-TD-24; 14.1-LS-4; 6.1-TD;25; 6.1-TD-71; 19.1-LN-9; 12.1-RM-27; 12.1-RM-28.

117. 25.1-BV-16; 25.1-BV-6; 25.1-BV-7; 25.1-BV-8.

118. 17.1-JH-15.

119. 16.1-JH-3; 16.1-JH-4; 16.1-JH-5.

120. 9.1-PL-18; 9.1-PL-10; 9.1-PL-11; 9.1-PL-13; 9.1-PL-15; 23.1-SP-28;.

121. 16.1-JH-2; 23.1-SP-29; 5.1-CG-44; 14.1-LS-30; 23.1-SP-42.

122. 16.1-JH-31; 5.1-CG-50; 9.1-PL-12.

123. 16.1-JH-25; 16.1-JH-26; 16.1-JH-28; 16.1-JH-30; 16.1-JH-32; 16.1-JH-27.

124. 18.1-NW-28.

125. 9.1-PL-40; 9.1-PL-41; 9.1-PL-42; 9.1-PL-439.1-PL-16.

126. 17.1-JH-9.

127. 9.1-PL-65.

128. 9.1-PL-23.

129. 9.1-PL-14.

130. 5.1-CG-68.

131. 23.1-SP-50.

132. 1.2-LH-5; 16.1-JH-31.

133. 10.1-RP-19.

134. 6.1-TD-12.

135. 10.1-RP-58; 10.1-RP-59; 10.1-RP-60; 10.1-RP-61; 10.1-RP-62; 10.1-RP-63.

136. 12.1-RM-69; 12.1-RM-70; 12.1-RM-71; 12.1-RM-73; 7.1-RM-36; 12.1-RM-48; 12.1-RM-49; 2.1-BW-55.

137. 10.1-RP-5 ;19.1-LN-30.

138. 18.1-NW-31.

139. 23.1-SP-56; 24.1-JD-52; 21.1-AM-62.

140. 24.1-JD-55; 23.1-SP-55.

141. 10.1-RP-7.

142. 12.1-RM-3; 12.1-RM-1; 12.1-RM-2.

143. 23.1-SP-20; 23.1-SP-21; 23.1-SP-22; 23.1-SP-23; 18.1-NW-23; 24.1-JD-30; 3.1-JP-23; 14.1-LS-10; 23.1-SP-24; 19.1-LN-7; 19.1-LN-8; 21.1-AM-7; 24.1-JD-17; 24.1-JD-27; 17.1-JH-5; 5.1-CG-16; 7.1-RM-35; 17.1-JH-16; 7.1-RM-50; 1.1-LH-2; 3.1-JP-52; 10.1-RP-23; 23.1-SP-19..

144. 10.1-RP-28; 10.1-RP-29; 10.1-RP-30; 16.1-JH-14; 19.1-LN-3; 15.1-JH-39; 12.1-RM-21; 12.1-RM-22; 12.1-RM-23;12.1-RM-24; 12.1-RM-25.

145. 25.1-BV-29; 25.1-BV-30.

146. 10.1-RP-31.

147. 7.1-RM-8.

148. 17.1-JH-6; 10.1-RP-18; 7.1-RM-13; 5.1-CG-17; 1.1-LH-7; 7.1-RM-39; 7.1-RM-37; 1.1-LH-34.

149. 7.1-RM-29.

150. 3.1-JP-56; 3.1-JP-45; 25.1-BV-28.

151. 12.1-RM-74.

152. 2.1-BW-51; 2.1-BW-52; 2.1-BW-53; 19.1-LN-51; 13.1-JL-30; 2.1-RM-32.

153. 13.1-JL-31

154. 2.1-BW-54.

155. 8.1-KW-21; 8.1-KW-35.

156. 22.1-AC-19-A; 22.1-AC-23-A; 22.1-AC-20.

157. 4.1-MI-3; 18.1-NW-43; 21.1-AM-17; 24.1-JD-1.

158. 18.1-NW-69.

159. 11.1-AG-32.

160. 2.1-BW-40; 10.1-RP-44; 7.1-RM-33; 7.1-RM-34..

161. 16.1-JH-19; 16.1-JH-20.

162. 10.1-RP-42; 10.1-RP-43.

163. 2.1-BW-42; 12.1-RM-91.

164. 21.1-AM-42; 21.1-AM-43.

165. 21.1-AM-65.

166. 5.1-CG-4; 2.1-BW-38; 2.1-BW-39; 19.1-LN-14; 1.1-LH-40; 1.1-LH-41; 1.1-LH-44; 1.1-LH-46; 1.1-LH-48; 19.1-LN-16.

167. 4.1-MI-23; 6.1-TD-42.

168. 15.1-JH-27; 6.1-TD-41; 6.1-TD-43; 21.1-AM-38; 21.1-AM-39; 14.1-LS-28.

169. 25.1-BV-35; 25.1-BV-34

170. 15.1-JH-29.

171. 16.1-JH-15; 16.1-JH-16.

172. 4.1-MI-27; 4.1-MI-28; 4.1-MI-29; 4.1-MI-30; 4.1-MI-22.

173. 11.1-AG-27; 11.1-AG-28.

174. 4.1-MI-24; 4.1-MI-25.

175. 13.1-JL-11; 13.1-JL-9; 6.1-TD-67.

176. 15.1-JH-28.

177. 18.1-NW-59; 14.1-LS-35; 24.1-JD-32; 24.1-JD-33; 24.1-JD-34; 17.1-JH-8; 17.1-JH-10; 10.1-RP-33; 10.1-RP-34; 10.1-RP-35; 10.1-RP-36; 10.1-RP-37; 10.1-RP-38; 10.1-RP-40; 10.1-RP-41; 3.1-JP-27; 3.1-JP-28.

178. 22.1-AC-13; 4.1-MI-59; 22.1-AC-14; 3.1-JP-53; 3.1-JP-2..

179. 13.1-JL-20; 19.1-LN-19.

180. 8.1-KW-47; 8.1-KW-48; 14.1-LS-29; 13.1-JL-10; 8.1-KW-38; 8.1-KW-39; 4.1-MI-36.

181. 14.1-LS-25; 8.1-KW-46; 2.1-BW-41.

182. 23.1-SP-33-A; 23.1-SP-41; 23.1-SP-42-A; 23.1-SP-43; 23.1-SP-44; 23.1-SP-36; 23.1-SP-37; 23.1-SP-38; 23.1-SP-39; 23.1-SP-40; 23.1-SP-34.

183. 23.1-SP-35.

184. 10.1-RP-45.

185. 18.1-NW-47; 18.1-NW-48; 18.1-NW-50; 13.1-JL-21.

186. 25.1-BV-12; 11.1-AG-35; 25.1-BV-17-A; 25.1-BV-18; 25.1-BV-19; 25.1-BV-20; 25.1-BV-21; 25.1-BV-14 18.1-NW-75.

187. 25.1-BV-15; 25.1-BV-17.

188. 5.1-CG-43.

189. 20.1-JS-15.

190. 4.1-MI-26.

191. 21.1-AM-46.

192. 18.1-NW-76; 18.1-NW-77; 18.1-NW-30; 18.1-NW-60; 1.1-LH-2612.1-RM-92; 12.1-RM-93.

193. 24.1-JD-42.

194. 18.1-NW-36; 18.1-NW-37; 18.1-NW-68; 18.1-NW-70; 18.1-NW-74; 2.1-BW-37; 18.1-NW-35; 14.1-LS-38; 21.1-AM-57; 18.1-NW-34; 18.1-NW-90.

195. 18.1-NW-67; 18.1-NW-72; 18.1-NW-73; 21.1-AM-45.

196. 14.1-LS-27.

197. 18.1-NW-94.

198. 14.1-LS-26.

199. 18.1-NW-61.

200. 18.1-NW-66; 14.1-LS-56; 18.1-NW-91.

201. 20.1-JS-18; 6.1-TD-50.

202. 14.1-LS-33; 14.1-LS-34; 18.1-NW-96; 18.1-NW-97; 18.1-NW-92.

203. 19.1-LN-18; 6.1-TD-70; 19.1-LN-4; 19.1-LN-17; 25.1-BV-33; 5.1-CG-13; 20.1-JS-16; 20.1-JS-17.

204. 14.1-LS-40.

205. 24.1-JD-38.

206. 13.1-JL-23; 13.1-JL-24; 13.1-JL-25; 13.1-JL-26.

207. 21.1-AM-23; 21.1-AM-32.

208. 21.1-AM-36; 21.1-AM-37; 21.1-AM-34; 21.1-AM-35.

209. 1.1-LH-32; 6.1-TD-60; 1.2-LH-3; 15.1-JH-32; 14.1-LS-41; 14.1-LS-42; 7.1-RM-15; 3.1-JP-38; 6.1-TD-44; 19.1-LN-28; 19.1-LN-26; 10.1-RP-46; 10.1-RP-47; 13.1-JL-3; 25.1-BV-36; 2.1-BW-46.

210. 21.1-AM-63.

211. 25.1-BV-37; 25.1-BV-38.

212. 8.1-KW-53.

213. 18.1-NW-38; 12.1-RM-94; 7.1-RM-42; 3.1-JP-41; 2.1-BW-43; 2.1-BW-45; 2.1-BW-48; 2.1-BW-49; 11.1-AG-36; 14.1-LS-43; 24.1-JD-40; 24.1-JD-41; 21.1-AM-40; 6.1-TD-54; 6.1-TD-55; 6.1-TD-56; 6.1-TD-57; 6.1-TD-58; 6.1-TD-59; 1.1-LH-27; 1.1-LH-28.

214. 4.1-MI-45.

215. 21.1-AM-58.

216. 20.1-JS-19.

217. 6.1-TD-20; 6.1-TD-21; 6.1-TD-22.

218. 20.1-JS-20; 20.1-JS-21.

219. 16.1-JH-17; 16.1-JH-18; 10.1-RP-50; 3.1-JP-39; 2.1-BW-44; 19.1-LN-27; 10.1-RP-48; 10.1-RP-49; 6.1-TD-48; 6.1-TD-49.

220. 8.1-KW-49; 8.1-KW-50; 8.1-KW-51; 8.1-KW-52; 9.1-PL-22; 3.1-JP-40; 2.1-BW-47; 24.1-JD-35;14.1-LS-48.

221. 18.1-NW-79; 19.1-LN-25; 19.1-LN-24; 22.1-AC-15; 6.1-TD-52; 9.1-PL-23; 12.1-RM-97; 6.1-TD-45; 6.1-TD-64.

222. 18.1-NW-45; 24.1-JD-36; 24.1-JD-37; 18.1-NW-78; 21.1-AM-47; 18.1-NW-44; 6.1-TD-47; 21.1-AM-50; 21.1-AM-24-A..

223. 9.1-PL-24; 9.1-PL-25; 9.1-PL-26; 9.1-PL-27; 9.1-PL-28; 16.1-JH-22; 6.1-TD-53; 17.1-JH-11; 17.1-JH-12; 5.1-CG-70; 5.1-CG-69; 9.1-PL-20; 1.1-LH-10; 1.2-LH-11; 10.1-RP-51.

224. 22.1-AC-16; 10.1-RP-52; 10.1-RP-53; 10.1-RP-54; 12.1-RM-39; 5.1-CG-65; 5.1-CG-66; 23.1-SP-45; 5.1-CG-56; 1.2-LH-2; 7.1-RM-46; 7.1-RM-43; 7.1-RM-45; 7.1-RM-47; 15.1-JH-30; 15.1-JH-31; 23.1-SP-46; 23.1-SP-18; 5.1-CG-61; 5.1-CG-63; 5.1-CG-71; 5.1-CG-67; 5.1-CG-64; 23.1-SP-48; 16.1-JH-21; 22.1-AC-17.

225. 11.1-AG-37; 1.2-LH-4; 9.1-PL-29.

226. 6.1-TD-63; 6.1-TD-61; 6.1-TD-62; 5.1-CG-36.

227. 6.1-TD-51; 5.1-CG-53; 1.2-LH-1; 5.1-CG-51; 5.1-CG-52.

228. 9.1-PL-21; 5.1-CG-48.

229. 5.1-CG-58; 5.1-CG-60; 5.1-CG-59.

230. 5.1-CG-57; 5.1-CG-84; 23.1-SP-47; 10.1-RP-56; 3.1-JP-15.

231. 5.1-CG-54; 5.1-CG-55; 7.1-RM-44.

232. 1.2-LH-6; 1.2-LH-7; 1.2-LH-9; 1.1-LH-8.

233. 12.1-RM-95; 1.2-LH-8.

234. 5.1-CG-62; 12.1-RM-98.

235. 12.1-RM-99.

236. 9.1-PL-9.

237. 10.1-RP-39; 3.1-JP-26; 5.1-CG-37; 5.1-CG-31; 12.1-RM-82; 1.1-LH-25; 5.1-CG-33; 3.1-JP-31; 10.1-RP-32; 2.1-BW-34; 2.1-BW-31; 2.1-BW-32; 2.1-BW-33; 2.1-BW-35; 11.1-AG-26; 3.1-JP-35; 2.1-BW-36; 11.1-AG-31; 8.1-KW-45; 12.1-RM-79; 14.1-LS-31; 5.1-CG-35; 6.1-TD-38; 7.1-RM-32; 2.1-BW-30.

238. 5.1-CG-34; 6.1-TD-65; 6.1-TD-36; 6.1-TD-66.

239. 10.1-RP-6.

240. 4.1-MI-16; 4.1-MI-17; 5.1-CG-3; 5.1-CG-14; 5.1-CG-1; 7.1-RM-27.

241. 7.1-RM-28; 24.1-JD-2; 18.1-NW-33; 12.1-RM-5; 18.1-NW-26; 10.1-RP-1; 10.1-RP-2; 10.1-RP-4; 2.1-BW-11; 17.1-JH-2; 16.1-JH-1; 9.1-PL-1; 6.1-TD-14; 6.1-TD-15.

242. 3.1-JP-5; 3.1-JP-2; 3.1-JP-1; 14.1-LS-3; 14.1-LS-2; 14.1-LS-1; 2.1-BW-2; 2.1-BW-10; 2.1-BW-9; 2.1-BW-8; 2.1-BW-7; 2.1-BW-6; 2.1-BW-5; 2.1-BW-4; 2.1-BW-3; 18.1-NW-1; unpacked/analytical process

243. 11.1-AG-5; 11.1-AG-6; 11.1-AG-7; 11.1-AG-8; 11.1-AG-9.

244. 11.1-AG-15.

245. 22.1-AC-1; 2.1-BW-1; 22.1-AC-4; 10.1-RP-55; 3.1-JP-3; 3.1-JP-4; 25.1-JP-1; 25.1-BV-2; 25.1-BV-3; 25.1-BV-4; 25.1-BV-45; 13.1-JL-1; 13.1-JL-2; 25.1-BV-9; 25.1-BV-10; 25.1-BV-11; 25.1-BV-13; 25.1-BV-5; 11.1-AG-34; 15.1-JH-3; 15.1-JH-7; 6.1-TD-19; 24.1-JD-11; 11.1-AG-11; 11.1-AG-12; 11.1-AG-13; 11.1-AG-14.

246. 11.1-AG-19.

247. 18.1-NW-80.

248. 6.1-TD-46; 15.1-JH-1; 15.1-JH-2; 21.1-AM-60; 19.1-LN-15; 21.1-AM-25; 21.1-AM-26.

249. 8.1-KW-14.

250. 25.1-BV-44.

251. 20.1-JS-22.

252. 17.1-JH-13.

253. 25.1-BV-40; 25.1-BV-41; 25.1-BV-42; 25.1-BV-43; 22.1-AC-18.

254. 21.1-AM-9; 21.1-AM-51; 4.1-MI-19; 4.1-MI-20; 4.1-MI-21; 22.1-AC-22.

255. 15.1-JH-34; 15.1-JH-33; 15.1-JH-16; 15.1-JH-11; 15.1-JH-12; 15.1-JH-13; 15.1-JH-14; 15.1-JH-15; 7.1-RM-26.

256. 19.1-LN-29; 8.1-KW-27; 8.1-KW-22; 14.1-LS-23.

257. 12.1-RM-40; 12.1-RM-41; 12.1-RM-42; 12.1-RM-43; 18.1-NW-19; 18.1-NW-20; 18.1-NW-21; 18.1-NW-22.

258. 8.1-KW-28; 8.1-KW-25.

259. 4.1-MI-67; 14.1-LS-49; 4.1-MI-37; 4.1-MI-58.

260. 8.1-KW-1; 8.1-KW-2; 8.1-KW-3; 8.1-KW-5; 8.1-KW-6; 8.1-KW-7; 8.1-KW-8; 8.1-KW-9; 8.1-KW-4; 8.1-KW-10; 8.1-KW-12.

261. 16.1-JH-23; 16.1-JH-24.

262. 8.1-KW-11.

263. 23.1-SP-54.

264. 8.1-KW-18; 8.1-KW-19; 8.1-KW-20.

265. 7.1-RM-22.

266. 8.1-KW-16; 8.1-KW-15.

267. 4.1-MI-32; 4.1-MI-35; 14.1-LS-8; 4.1-MI-55; 4.1-MI-33; 4.1-MI-34.

268. 4.1-MI-68.

269. 8.1-KW-29; 8.1-KW-30.

270. 13.1-JL-32; 13.1-JL-33.

271. 4.1-MI-18; 8.1-KW-13.

272. 23.1-SP-49; 18.1-NW-81.

273. 21.1-AM-53; 21.1-AM-54.

274. 4.1-MI-60; 4.1-MI-62; 4.1-MI-63; 4.1-MI-64; 4.1-MI-65; 4.1-MI-66; 4.1-MI-61.

275. 9.1-PL-39; 23.1-SP-30; 9.1-PL-41-A; 14.1-LS-20; 14.1-LS-21; 14.1-LS-52; 14.1-LS-12.

276. 19.1-LN-13; 19.1-LN-36; 19.1-LN-37; 1.1-LH-10; 14.1-LS-50; 14.1-LS-51; 23.1-SP-31; 1.1-LH-11.

277. 8.1-KW-33; 8.1-KW-23; 8.1-KW-31; 8.1-KW-32; 8.1-KW-24.

278. 13.1-JL-28.

279. 13.2-JL-1

280. 15.1-JH-35; 19.1-LN-34; 13.1-JL-29.

281. 8.1-KW-26; 9.1-PL-3; 3.1-JP-24.

282. 13.1-JL-27; 13.1-JL-34.

283. 4.1-MI-4; 4.1-MI-6; 4.1-MI-7; 4.1-MI-8; 4.1-MI-9; 4.1-MI-43; 4.1-MI-44; 1.1-LH-45.

284. 3.1-JP-43; 10.1-RP-3; 20.1-JS-1; 3.1-JP-42; 3.1-JP-48; 3.1-JP-51; 3.1-JP-49; 3.1-JP-50.

285. 18.1-NW-83; 18.1-NW-84; 18.1-NW-85; 18.1-NW-86; 18.1-NW-87; 18.1-NW-88; 21.1-AM-52; 18.1-NW-82; 25.1-BV-39; 11.1-AG-18.

286. 22.1-AC-19; 22.1-AC-23; 22.1-AC-25; 22.1-AC-26; 22.1-AC-27; 22.1-AC-28; 22.1-AC-24.

287. 19.1-LN-39; 19.1-LN-40; 19.1-LN-42; 15.1-JH-20; 4.1-MI-41; 4.1-MI-38; 4.1-MI-39; 18.1-NW-89.

288. 11.1-AG-38; 11.1-AG-39; 14.1-LS-39; 18.1-NW-93; 14.1-LS-32.

289. 18.1-NW-65; 11.1-AG-10; 6.1-TD-37.

290. 4.1-MI-10; 4.1-MI-11.

291. 5.1-CG-72; 5.1-CG-73; 4.1-MI-31.

292. 13.1-JL-12; 13.1-JL-7.

293. 13.1-JL-18; 13.1-JL-13; 13.1-JL-14; 13.1-JL-15; 13.1-JL-16; 13.1-JL-17; 13.1-JL-19; 4.1-MI-40.

294. 7.1-RM-14; 15.1-JH-24; 18.1-NW-55; 11.1-AG-16; 11.1-AG-17; 15.1-JH-40; 15.1-JH-37;15.1-JH-38.

295. 21.1-AM-10.

296. 4.1-MI-54; 4.1-MI-12; 4.1-MI-46; 4.1-MI-48.

297. 20.1-JS-12; 20.1-JS-9.

298. 6.1-TD-1; 6.1-TD-2; 6.1-TD-3; 6.1-TD-4; 6.1-TD-5.

299. 4.1-MI-49; 4.1-MI-50; 4.1-MI-51; 4.1-MI-52; 4.1-MI-53.

300. 22.1-AC-21.

301. 21.1-AM-28-A; 21.1-AM-29; 21.1-AM-18; 21.1-AM-56.

302. 21.1-AM-12; 21.1-AM-71.

303. 21.1-AM-11; 21.1-AM-49; 7.1-RM-40; 21.1-AM-48.

304. 21.1-AM-14; 21.1-AM-15.

305. 21.1-AM-5; 21.1-AM-6; 21.1-AM-61; 21.1-AM-3; 21.1-AM-4; 21.1-AM-66; 21.1-AM-67; 21.1-AM-55; 21.1-AM-41; 21.1-AM-59.

Appendix F

Audit Report for Linda Larkin

Purpose of the Audit

This audit serves as a warrant of the quality of the research process and product of the following study: What is the meaning of security? : A constructivist inquiry into the context of information security policy development post 9/11. This study was conducted by Linda Larkin, doctoral candidate at Virginia Commonwealth University.

Audit Process

The audit process consisted of an initial meeting to define the scope of the audit and obtain materials for the audit, an initial review of materials, an in-depth audit of materials to evaluate the rigor of the research process and product.

Initial Meeting

Linda and I met for an initial meeting to define the scope of the audit and agree on materials needed for the audit trail. For the scope of the audit we agreed that a full audit of trustworthiness would be conducted to include dimensions of confirmability, credibility, dependability and transferability. We agreed that the dimension of tactical authenticity would not be audited due to the context of the inquiry and to the timing of the audit. Linda ended her data collection in December 2003 and returned to do a final member check in May of 2004. We were both concerned that the six month time period between data collection and follow up was not sufficient for evidence of tactical authenticity. Furthermore, the context of the inquiry, may be difficult for people to extract the change that occurred due to this research from ongoing dialogues they may engage in around this complex and rapidly changing phenomenon. The audit consists of a full audit of trustworthiness and a modified audit of authenticity to include dimensions of fairness,

ontological, educative and catalytic authenticity. We agreed on the timeline and format for the report of audit findings. We also agreed on procedures for securing the audit materials while the audit was being conducted.

Linda provided me with the following audit materials:

- Journals: Reflexive journal, methodological journal, and peer review
- Data Collection Materials: Chronological set of field notes for 25 interviews, transcriptions of 25 interviews, and all documents with document summary forms attached
- Data Analysis Materials: Schemata of categories, coding rules, full set of unitized and sorted index cards
- Participant Materials: Copies of informed consent, journal of member checks and final member checks with participants
- Draft and Final Case Study

Initial Review of Materials

The initial review of materials serves as an overall check that the research has been conducted following guidelines of constructivist inquiry. This review of materials took approximately two hours in which I verified that items were complete and asked the following questions:

- Did the inquiry take place in a natural setting?
- Is the context of the inquiry apparent?
- Is prolonged engagement in the setting apparent?
- Are the data collected congruent with constructivist methods?

Upon this review I concluded the materials provided did give an indication that the context was government, private industry, non-profits, and educational institutions at the state and federal level. The inquiry took place in natural settings, the offices and workplaces of the participants. The data collection began in April and continued through December

evidence of prolonged engagement and there was clear evidence of the use of interviews, researcher transcription, and reliance on participant words as the data source.

Auditing Dimensions

Two dimensions of rigor will be addressed in this audit: trustworthiness and authenticity. A description of the dimension and criteria used as a guideline for this audit are outlined in the table below.

Dimension	Description	Evaluation Criteria
Trustworthiness - Credibility	How well do data represent stakeholders' perspectives	Use of member checks at the end of each interview/data collection Prolonged and persistent observation Inclusion of all data in analysis Peer review and use of reflexive journal to distinguish researcher constructions from participant constructions
Trustworthiness -Confirmability	How well findings are gounded in data logic of analysis is developed	Review of audit trail from findings to raw data Documentation in methodological journal of decision rules for categorization and connection between themes Review of categories and data units
Trustworthiness -Dependability	How well research attends to the assumptions of constructivist methodology	Review of peer review, reflexive and methodological journal to show how decisions are made, ensure sampling is purposive, data saturation decisions are substantiated, and document evidence of a hermeneutic circle, expose researcher bias/values
Trustworthiness -Transferability	How well readers can connect to the final case study	Thick description of details and context of security and technology policy Engaging writing style
Authenticity – Fairness	Managing power and multiple perspectives	Sampling strategy Member checks Use of all data; fair representation of all perspectives Researcher attention to negotiations made in handling emergence of research process

Ontological Authenticity	Increased understanding among participants of the complexity of the phenomena	Researcher ability to reflect on alternative views and provide feedback to participants to increase alternative understandings (creation of hermeneutic circle) Documentation of changes in interview schedule that show cross pollination of constructions of security, technology and policy
Educative Authenticity	Empathy or appreciation for different understandings	Examination of follow up interviews to elicit appreciations or understandings of alternative views Researcher ability to introduce different constructions in respectful fashion (maintenance of quality hermeneutic circle)
Catalytic Authenticity	Participants' engagement in possible or actual plans related to phenomena of inquiry	Documentation of instances of interest in acting on the developing meanings, willingness to be involved in activities related to change, transformation in constructed meanings and experiences in the context Follow up to assess extent of change or action related to research

Statement of Findings

Trustworthiness

Credibility

In reviewing the documents available for the audit I sought evidence that strategies in the research design were used to enhance credibility. Linda did an excellent job ensuring that participants words and meanings were accurately represented. Evidence of member checks was found for all participants at the close of each contact. Linda provided each participant a full transcript of the interview for review. She allowed participants to edit the documents and then updated her transcripts accordingly; tracing several of these changes indicated Linda had made the recommended edits. Most participants fully

reviewed the transcripts and commented on the accuracy of her transcriptions, demonstrating their commitment to the research process and her skills in capturing what they said. Final member checks were available for 5 out of 25 participants. All of these participants indicated the case study accurately captured their perspective. Evidence of peer debriefing was indicated through the peer review journal. Peer review was ongoing throughout the research. Both the peer review and reflexive journal indicate researcher change in awareness and indication of an awareness of her own biases coming from a community college setting. Separation of participant construction from researcher construction is evident in the construction of the case study as well as comments made throughout the reflexive journal. Evidence of prolonged and persistent observation was found in the length of time spent in context and the development of themes over close to a year long period in the reflexive and methodological journals.

No strategies for triangulation of data were apparent. Documents were collected but not included in the analysis. Data inclusion was checked by reviewing units that were not categorized. No units were left uncategorized.

Confirmability : Findings Grounded in Data

Through my examination of the case study and tracing data backwards from the case study to raw field notes and forwards from raw field notes to the case study I sought to evaluate if the findings as presented are grounded in the data. From the case study I randomly sampled 25 of the references and traced them to unitized data. I found that in most cases, the audit trail was complete, except for areas where duplicate cards had not been provided. Since Linda's audit trail was not connected between the raw notes and

expanded notes I carefully compared four sets of field notes with an interview for correspondence and then traced several items in the interview up to the case study. The field notes correspond to the interview in terms of language and order of questions. Overall, the data in the results were identifiable back to the raw data and incorporate the words and meaning of the participants.

Confirmability: Logic

Through reviewing the categories and data contained within, the category labels appeared to accurately describe the concepts in the data to me. The final schemata contained four meta categories and four major categories which were well defined and distinct. Each major category contained from six to eleven subcategories. Some overlap seemed to exist between main categories among subcategories such as I.c. Protection with II.b Security Programs/Policy and II.e. Protecting information as it is disseminated also between categories II.e.5 Developing Security Policy and III.f. Policy Making Process. The challenge with this phenomenon is the subtle differences of meaning in security, technology and policy making that Linda explored which contribute to subtle differences in categories. A sampling of units within subcategories and categories demonstrated congruence. In less than 10% of the units sampled did I question the congruence with the assigned category. Overall,the data units were clear examples of the concept expressed by the category and the category label and decision rules reflected the data units.

Confirmability: Usefulness of Structure

Three levels of analysis were documented with larger categories abstractions of the smaller categories. One map of the categories was reviewed that contained the meta categories and stakeholding groups. No maps were available that related the subcategories or four main categories. The lack of a clear picture of the relationship between categories and their connection to the meta-categorical picture makes a determination of the usefulness of the analytical structure difficult. Although both the meta level of analysis and the main categories seem logical on their own, the connection between the two was not readily apparent. Throughout the journals, however, is attention to themes and categories and renditions of the categorical structure. I can only assume that the boundaries of information security policy making are so flexible at this point they provide a challenge for analysis; and a challenge for me the auditor to comprehend. Because I am not able to fully assess this dimension my warrant of confirmability does not include the usefulness of the structure.

Dependability

Linda addressed the issue of data saturation with her peer reviewer after determining that her participants were nominating similar participants; which served as a proxy for data redundancy. Linda's sample expanded to include private industry and her growing understanding of the importance of this stakeholding group was reflected in her methodological and peer review journal. She also reflected on the need to sample participants from smaller and larger educational institutions. There was no indication of the proportion of participants sampled from each of the four stakeholding groups:

government, non-profit, private sector and university but her coding did allow me to assess that 12 participants were technologists, 11 policy makers and 2 from agencies relevant to policy making.

There was no evident bias towards specific participants or a convergence of the data to her questions. On the contrary Linda's questions shifted over the course of the research to include an emphasis on the language and framing of policy. Linda's questions were open ended and elicited in-depth responses. Emergence was noted through the shift in questions, changing themes, and introduction of new stakeholding group. Evidence of a working hermeneutic circle is difficult to obtain in any audit. The most notable evidence is the change in the interview guide. Linda did document several follow up questions to participants, but most of the exchange of perspectives appeared to occur at the final member check.

Transferability

Evidence of transferability is found in the details of the case study report that clearly distinguish the multiple voices involved in information security policy. The context of this policy making, with its complexity and multiple, competing voices is clear from the writing of the case study.

Authenticity

In order to assess this area I looked specifically for member interactions that reflected on the process of the research. With regards to fairness, I found evidence of ongoing member checking for all participants and a final member check for five participants. Linda indicated that the final member check included a participant from each

stakeholding group. Other evidence of fairness includes an informed consent process for all participants. The use of multiple characters in her final case study also speaks to fairness in her attempts not to oversimplify or lump together the perspectives of too many participants.

Several other comments were made by participants that indicated authenticity. Ontological authenticity was most noticeable in both researcher reflections on her changing awareness of the complexity of this phenomenon, subsequent changes in interview protocol, and participant responses. Participants' comments both during interviews and at the final member check indicated an increased awareness of the complexity of information security policy indicating that the research and the questions Linda was asking were needed and that the issue was complex. Educative authenticity was also apparent. Participants who read the completed case study all commented that they had gained insight from an alternative construction. One participant was intrigued with the discussion of trade-offs and would have liked to extend this conversation with some of the other participants. Another discussed how they had not been aware of physical security issues concurrent with information security. With regards to catalytic authenticity, one participant acknowledged that they had not been aware of the issues of information security within higher education and this would change his interactions with this community.

Summary

Based on the abovementioned materials, criteria and findings, I can attest to credibility, confirmability, transferability and dependability of the case study, entitled, What is the meaning of security? : A constructivist inquiry into the context of information security policy development post 9/11.

Kate Didden June 30, 2004

Vita

Linda F. Larkin received a B.A. in English from Richmond College of the City University of New York in Staten Island, NY and an M.S. in Library Service from Columbia University in New York, NY. She is Dean of Learning Resources at Germanna Community College in Fredericksburg and Locust Grove, VA and an adjunct faculty member at the University of Richmond. Linda has also guest lectured at Mary Washington College, Old Dominion University, and Virginia Commonwealth University.